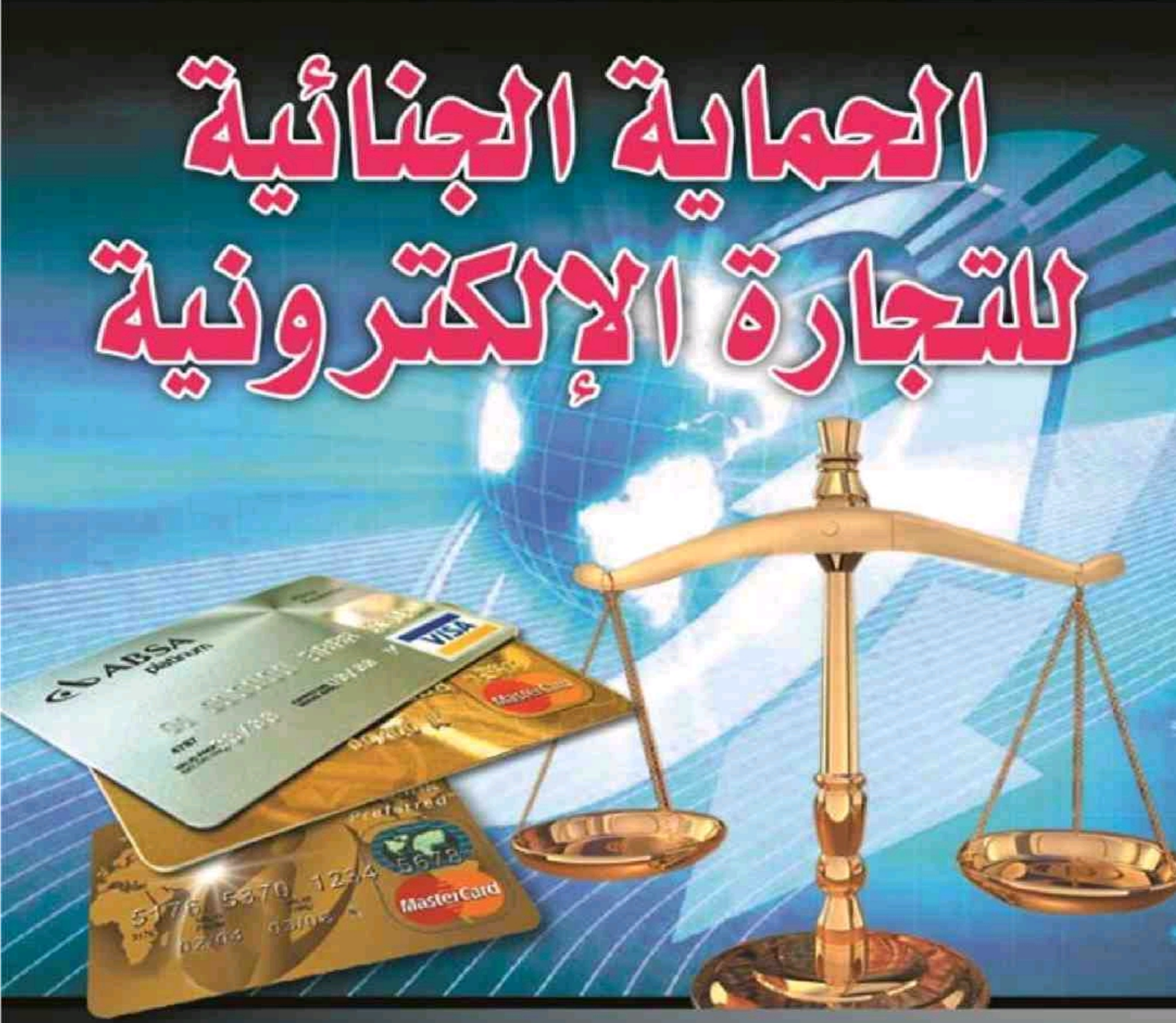
الحماية الجنائية للتجارة الإلكترونية



القاضي الدكتور

محمد عبيد الكعبي

الناشر

دار النهضة العربية

٣٢ شارع عبد الخالق ثروت - القاهرة

٢٠١٠

بسم الـلـه الرحمن الرحيم

﴿ قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ﴾ [1]

صدق الـلـه العظيم

(1) الآية رقم 32 من سورة البقرة

إهداء إلى ..

الإمارات... حكومة... وشعبًا.

والدي... ووالدتي...

زوجتي... أولادي... بناتي.

إخواني... أخواتي.

أصدقائي... وزملائي.

إيمانًا بدورهم وعرفانًا بفضلهم أهدي هذا الكتاب...

الحمايـــــة الجنائيــــة للتجارة الإلكترونية

المستشار الدكتور
محمـــد عبيـــد الكعبـــي

2010

الناشر
دار النهضة العربية

الحماية الجنائية للتجارة الإلكترونية

أولا: موضوع البحث وأهميته:

إذا استعرضنا التاريخ الاقتصادي سنجد فيه ملامح واضحة لعصرين إنتاجيين أساسيين تلاحقا على العالم، هما العصر الزراعي والعصر الصناعي، برزت خلالهما مقدمات تشكل عصرًا اقتصاديًا ثالثًا يطلق عليه البعض عصر اقتصاد المعلومات، وهذا الاقتصاد وضع عالمي مترابط يغطي معظم المجالات، لذا فإنه عصر العولمة، إنه يتطلب سرعة فائقة في التجاوب، ويعتمد على التقنيات العالية القادرة على توفير هذا المستوى المرتفع من سرعة التجاوب؛ لذا فإنه عصر التقنية، إنه اقتصاد غير منظور يهتم بالمعرفة والأفكار المبدعة؛ لذا فإنه عصر العقل المبدع[1].

فقد أفرز التطور التقني نوعًا جديدًا من الاقتصاد هو الاقتصاد الرقمي الذي تجسد في ظهور التجارة الإلكترونية والتي خرجت من رحم شبكة الإنترنت، تلك الشبكة التي نشأت عن عملية تزاوج بين التقنية والمعلومات، والتي دفعت العالم لتقدم نوعي جديد يضعه في القرن الحادي والعشرين، ومع التطور التكنولوجي الهائل في قطاع المعلومات والاتصالات انتشرت تلك التجارة بشكل متزايد ومستمر في كل أنحاء العالم.

وترتبط التجارة الإلكترونية بمستوى متطور من التقنيات الخاصة بالحاسب الآلي وملحقاته، وبقدر تقدم الدول في المجال التقني يكون دورها في هذه التجارة بوصفها منتجًا أو بائعًا، ولهذا ترتبط التجارة الإلكترونية بالتقدم العلمي ارتباطًا وثيقًا، وتحتاج إلى قواعد قانونية خاصة

(1) محمد بن راشد آل مكتوم، رؤيتي التحديات في سباق التميز، موتيفيت للنشر، 2006، ص 25.

لحماية كافة معاملاتها، وضمان تطورها وازدهارها على المستويات الدولية والإقليمية والوطنية.[1]

وتتميز التجارة الإلكترونية بأنها وسيلة غير مسبوقة للوصول إلى أسواق العالم في أسرع وقت ممكن بدون التقيد بمكان ما أو بأشخاص معينين، ورغم هذا التميز فإن أمام هذا القطاع أيضًا تحدياته ومعوقاته التي تهدد النشاط التجاري الذي يتم عبر شبكات الاتصال الحديثة، كالجرائم المعلوماتية والقرصنة التي تمثل تهديدًا حقيقيًا لنجاح هذه الأعمال في المستقبل، مما يقتضي بناء تقنية تؤمّن وتحمي بيانات التجارة الإلكترونية وأموالها، عبر أطر تشريعية تكفل تحقيق الحماية الجنائية لهذه التجارة.

ويمثل الإجرام المعلوماتي أبرز هذه العوائق، خصوصًا ذلك الإجرام المرتبط باختراق المواقع التجارية على شبكة الإنترنت، أو الدخول غير المشروع عليها، أو تقليد بعض محتوياتها المحمية بقوانين حماية الملكية الفكرية، أو تلك المتعلقة بانتهاك حرمة البيانات الاسمية أو الشخصية للمتعاملين في التجارة الإلكترونية والمرتبطة بالمعاملات المالية لهذه التجارة، أو الاعتداء على التوقيع الإلكتروني، أو على حقوق الملكية الفكرية سواء للمؤلفين أو العلامات التجارية.

ويعتبر موضوع الحماية الجنائية للتجارة الإلكترونية من الموضوعات المهمة التي فرضها الواقع والمستقبل، وله أهمية بالغة من الناحيتين النظرية والعملية على حد سواء، فمن الناحية النظرية يعالج الموضوع مفهوم الحماية الجنائية لنظام التجارة الإلكترونية من حيث مواقعها وأموالها وبياناتها وأطرافها وحقوق الملكية الفكرية، والتي قد يهدد الاعتداء عليها

(1) Joffery F.Beatty & Susan S. Samuelson, Essentials of Business law, 2nd Edition thomson, , 2005, p808.

الثقـة في هذا النوع من التجارة.

ومن الناحية العملية التطبيقية فـالواقع يؤكـد تزايـد حركــة التجــارة الإلكترونيـة في العـالم بأسره، فمستخدمو هذا النوع مـن التجـارة يـزدادون بعــشرات الملايــين، وقــد تضـاعفت هـذه الزيادة مع انتشار اسـتخدام شبكة الإنترنت والبريـد الإلكتروني.

وتتمثل أهمية التجارة الإلكترونية في عصرنا الحاضر في أنها تشكل 20% من مجمـل التجـارة العالمية[1].

وتشير الدراسات المتخصصة في هذا المجال والصادرة من مجلس الوحـدة الاقتصـادية التـابع لجامعة الدول العربية أن معدل نمـو التجـارة الإلكترونية العربية يتم بنسبة 15% مقابـل نسـبة 30% كمعدل للنمـو العالمي، وهو أمر يتطلـب ضرورة أن تسـعى الـدول العربيـة جاهـدة نحـو صياغة جديدة لتشريعاتها، أو بالأحرى سن قوانين جديدة كي تنظم هذه النــوعية المتنامية مـن التجـارة، وتحـول دون تعرض بياناتها وأموالها للقرصنة أو الإجرام المعلوماتي، لا سـيما وأن الـدول العربية تتمتـع بفـرص هائلـة في مجـال صـناعة البرمجيـات ونظــم المعلومـات وابتكـار الـبرامج وتطويرها، مما يستدعي إيجاد أساليب لحمايتها.

ويؤكد أهمية هذا الموضوع اعتبار القوانين المقارنة تلك الحماية مصلحة قوميـة واجتماعيـة تستحق التدخل لتحقيقها عن طريق إيجاد الأدوات القانونية اللازمـة لتـوفير الحمايـة لعمليـات التجارة الإلكترونية، وذلك بتجريم

(1) د. كامران الصالحي، الطبيعة القانونية لمسئولية خدمات التصديق، مؤتمر المعـاملات الإلكترونيـة (التجـارة الإلكترونيـة، الحكومـة الإلكترونيـة) 19- 25 مـايو 2009، جامعـة الإمـارات، مركـز الإمـارات للبحـوث والدراسات الإستراتيجية، ج2، ص 617.

الأفعال المتمثلة في الاعتداء على مواقع وأموال وبيانات وأطراف تلك التجارة[1]، فقد اهتمت التشريعات الأجنبية والعربية اهتمامًا متزايدًا بموضوع التجارة الإلكترونية والقوانين ذات الصلة بها، فعلى المستوى الدولي قامت لجنة الأمم المتحدة لقانون التجارة الدولية بإصدار قواعد نموذجية موحدة للتجارة الإلكترونية (الأونسيترال) بهدف توحيد القوانين والتنسيق بين الدول، ومن أهم هذه القواعد القانون النموذجي بشأن التجارة الإلكترونية الصادر من اللجنة عام 1996، والقانون النموذجي بشأن التوقيعات الإلكترونية، وقد اعتمدت الجمعية العمومية للأمم المتحدة هذه القواعد.

كما اهتم المشرع الأوروبي بموضوع التجارة الإلكترونية، فأصدر مجموعة من التوجيهات كان أبرزها التوجيه الأوروبي الصادر عام 2000 بشأن التجارة الإلكترونية، وتوقيع الدول الأوروبية على اتفاقية الجريمة الافتراضية (بودابست).

وعلى صعيد الدول هناك القانون الفرنسي المتعلق بتكنولوجيا المعلومات والتوقيع الإلكتروني، والذي نص على بعض التعديلات فيما يخص قانون الإثبات، وهناك أيضًا القانون الأمريكي الموحد الخاص بالتجارة الإلكترونية.

وفي دولة الإمارات العربية المتحدة صدر القانون الاتحادي رقم 2006/1 في شأن المعاملات والتجارة الإلكترونية، والقانون الاتحادي رقم 2006/2 في شأن مكافحة جرائم تقنية المعلومات، كما سبق وأصدر حاكم

---

(1) د. مدحت عبد الحليم رمضان, الحماية الجنائية للتجارة الإلكترونية, دار النهضة العربية، 2001، ص 35 ,
وفي المعنى ذاته: د. شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، 2007م، ص 29.

إمارة دبي القانون رقم 2 لسنة 2002 في شأن المعاملات والتجارة الإلكترونية.

كما تعد الجمهورية التونسية أول دولة عربية تصدر قانونا في هذا المجال حينما أصدرت في 9 أغسطس 2000 القانون الخاص بالمبادلات والتجارة الإلكترونية.

ونهدف في هذا البحث تحديدًا تناول موضوع الحماية الجنائية للتجارة الإلكترونية دراسة تأصيلية تحليلية مقارنة، نظرًا لما لهذا الموضوع من أهمية قصوى بسبب تزايد حجم التجارة الإلكترونية وانتشار التعامل بها من خلال شبكة الإنترنت.

ثانيًا: إشكاليات البحث:

يتناول هذا البحث العديد من المشكلات القانونية التي سنحاول معالجة أبعادها وإيجاد حلول لها، منها أن التقنية أحيانًا ما تكون غريبة على القانونين، لعدم فهم طريقة عملها بسهولة وعدم استيعابها بالسرعة اللازمة، مما ينتج عنه البطء الشديد في تنظيمها.

كما أن هذه التجارة وباعتبار أنها حديثة - وخاصةً على مجتمعاتنا العربية - فقد تعرضت للعديد من المشكلات العملية، كان أهمها ثقة المستهلك ومدى اطمئنانه إلى التسوق دون المعاينة المادية للسلعة كما هو متبع أثناء التعامل بالمتجر العادي، بالإضافة إلى إمكانية اختراق بيانات هذه التجارة على الشبكة أو إساءة استعمالها.

وتثير التجارة الإلكترونية - باعتبارها تجارة بلا حدود - مشكلة القرصنة ونسخ البرامج وتقليدها، ومشكلة الهاكرز المتمثلة في الدخول غير المشروع على الأنظمة والبرامج، ومشكلة تزوير المستندات والسجلات الإلكترونية، والاعتداء على التوقيع الإلكتروني، وعلى شهادات

المصادقة الإلكترونية، والسطو على العلامات التجارية والمواقع، وهـذه المشـكلات تعتبر التحدي الأصعب في مجال التجارة الإلكترونية.

فالتعاقد عبر وسـائل إلكترونيـة يحتـاج إلى تنظيم قـانوني لآليـاتها وقواعدها السياسية والتشريعية والضريبية والجمركيـة، مما من شأنه أن يسـاهم في تطوير هذه التجارة وازدهارها.

ويعد موضوع التجارة الإلكترونية من الناحية القانونية من الموضـوعات المتشعبة لارتباطه بعدة نواح مدنية وتجارية واقتصادية وجنائية، بالإضافة إلى اتصالها بالتقنية, وبالتالي لا نستطيع الحديث عن الحماية الجنائية للتجارة الإلكترونية بمنأى عن هذه النواحي.

ثالثا: سبب اختيار الموضوع:

تناول البحث موضوع الحماية الجنائية المقررة لنظـام التجـارة الإلكترونيـة مـن خـلال دراسـة مقارنـة تستهدف بيان توجهـات المشـرع العربي والفقه والقضاء الدوليين في هـذا الشـأن نظرًا لحداثة التجربة في البلاد العربية، فقد وجد أنـه مـن الملائـم البحـث عـن نظـام قـانوني لحمايـة هذه التجارة في ظل الخصوصية الاقتصادية التي تعيشها المنطقة العربيـة، وفـي سـبيل ذلـك قمنا بالتعريف بالتجارة الإلكترونيـة وتطورهـا في الـدول العربيـة وبعـض الـدول خـارج المنطقة العربية، بالإضـافة إلى بعـض التعريفـات الفقهيـة، مـع بيـان التهديـدات التـي تواجـه التجـارة الإلكترونيـة والمتمثلـة في اختـراق مواقع هـذه التـجارة علـى شبكة الإنترنت، وانتهـاك نظـام الحمايـة السرية، وإتلاف المواقع أو تدميرها بالوسـائل المختلفـة، بالإضـافة إلى مشـكلات أداة الوفـاء الإلكترونيـة، ووضـع سياسـة لحمايـة المسـتهلك تراعـي المعطيـات الاقتصـادية والاجتماعيـة.

وبحثنا بعد ذلك كيفية توفير الحماية الجنائية لهذه التجارة في ظل المخاطر التي تهددها، على نحو يساعد على نموها وتطورها، ولم نقتصر على معالجة الحماية الجنائية بتجريم الأفعال التي تعد اعتداءً على أموال هذه التجارة ونظامها وعقاب مرتكبي هذه الأفعال، بل أوردنا ضرورة حمايتها اقتصاديًّا، وتقنيًا، ومدنيًا.

وكان اختيارنا لهذا الموضوع ابتغاء الوصول إلى بعض الحلول التشريعية التي تحقق الأمان لأطراف هذه التجارة[1]، كما نحاول من خلال هذه الدراسة بحث مدى إمكانية تطبيق القواعد القانونية التقليدية، ومدى ضرورة سن تشريعات جديدة خصوصًا المتعلقة بوضع الضوابط الكفيلة بحماية أطراف هذه التجارة ووسائلها أمام قوة المجرم المعلوماتي وقدراته.

وقد ساعدنا في هذا البحث ظهور بعض الدراسات القريبة من هذا الموضوع في الفقه العربي في السنوات الأخيرة, وخاصة كتاب "الحماية الجنائية للتجارة الإلكترونية" لأستاذنا الدكتور "مدحت عبد الحليم رمضان", ومؤلف "الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت" لأستاذتنا الدكتورة "هدى حامد قشقوش", وهما من أول من كتب في هذا المجال، وقد ساعدا في نشر ثقافة قانون الإنترنت في الدول العربية, بالإضافة إلى دور باقي القانونيين في هذا المجال.

وقد تم الاستعانة بالعديد من الدراسات الأجنبية في هذا المجال, كما حاولنا الاستفادة مما تتيحه شبكة الإنترنت من المعلومات والمراجع

---

(1) د. عصام أنور سليم, خصائص البيع الدولي وفقا لاتفاقية الأمم المتحدة بشأن البيع الدولي للبضائع المبرمة في فيينا سنة 1998، منشأة المعارف، 2004، ص 7.

والأحكام المقارنة في مجال الدراسة, بالإضافة إلى عضويتنا في لجنة الخبراء العرب المكلفة بقرار من وزراء العدل بإعداد قانون عربي استرشادي للتجارة الإلكترونية, وقانون عربي استرشادي للإثبات بالوسائل الحديثة, ولجنة الخبراء المكلفة بقرار من وزراء الداخلية والعدل العرب بإعداد مشروع اتفاقية عربية موحدة للجريمة المعلوماتية.

رابعًا: منهج البحث:

فرضت حداثة الموضوع وعدم وجود قواعد محددة قائمة في تشريعات العديد من الدول منهج الدراسة، فكان اختيارنا للمنهج التحليلي المقارن من خلال التعرض بالشرح التفصيلي لأهم الموضوعات التي تحتاج إلى معالجة تشريعية والتي تشكل عائقًا قانونيًا أمام تطور التجارة الإلكترونية، ثم أتبعنا ذلك ببعض الأحكام القضائية من دول مختلفة، مع إبراز النتائج التي توصلنا إليها من خلال ذلك التحليل، كما قمنا بمقارنة النظم المختلفة من خلال دراسة القانون المصري والإماراتي وقوانين أخرى دولية ووطنية كالقانون الفرنسي والأمريكي، وقد اكتملت دراستنا المقارنة لهذه القوانين المختلفة من خلال دراسة النصوص الجنائية وأحكام القضاء.

خامسا: خطة البحث:

تتطلب الحماية الجنائية للمعاملات الإلكترونية حماية مواقع التجارة الإلكترونية من جرائم الدخول غير المشروع، وحماية أموال التجارة الإلكترونية من جرائم السرقة والنصب والاعتداء على بطاقات الدفع الإلكتروني والتزوير، وإلى جانب ذلك فإنها تتطلب حماية حقوق الملكية الفكرية لعلاقتها بالتجارة الإلكترونية، ونظرًا لأن التجارة الإلكترونية قسم من أقسام شبكة الإنترنت فكان من الضروري

دراسة التنظيم القانوني لشبكة الإنترنت، ولما كانت الدراسات الحديثة ما زالت لم تستوف كافة الجوانب المختلفة لهذا النوع من التجارة، فلزم تأصيل الدراسة ببحث تعريفها وأنواعها ومزاياها وعيوبها، مع بحث حمايتها اقتصاديًا وتقنيًا ومدنيًا، كل ذلك وفقًا للخطة الآتية:

فصل تمهيدي: التنظيم القانوني للإنترنت: بحثنا فيه ماهية شبكة الإنترنت ونشأتها وأقسامها وخصائصها والقانون المنظم لها.

الباب الأول: أساسيات التجارة الإلكترونية وحمايتها: وقد تناولناه من خلال ثلاثة فصول:

الفصل الأول: أساسيات التجارة الإلكترونية: تناولنا فيه ماهية التجارة الإلكترونية وخصائصها ومعوقاتها ومستقبلها.

الفصل الثاني: الحماية القانونية للتجارة الإلكترونية: بحثنا فيه المصلحة المحمية في التجارة الإلكترونية المتمثلة في حماية المواقع الإلكترونية للتاجر، وحماية المستهلك الإلكتروني، وحماية وسائل الدفع الإلكتروني، وتناولنا صور الحماية غير الجنائية، والحماية المدنية، والحماية الاقتصادية للتجارة الإلكترونية.

الفصل الثالث: تجارب التنظيم القانوني للتجارة الإلكترونية: تناولنا فيه التجارة الإلكترونية في المنظمات الدولية والإقليمية، وحماية التجارة الإلكترونية لدى أصحاب الشراكة في المجتمع المعلوماتي، وبحثنا مدلول أصحاب الشراكة، وإعلان جنيف 2003، وإعلان تونس 2005، كما تناولنا التجارة الإلكترونية في التشريعات الوطنية الأمريكية والأوروبية والعربية وبعض البلدان الأخرى.

الباب الثاني: الجرائم الواقعة على التجارة الإلكترونية: تناولنا فيه الجرائم الواقعة على المواقع الإلكترونية، والجرائم الواقعة على البيانات،

والجرائم الواقعة على وسائل التجارة الإلكترونية، والجرائم الواقعة على الملكية الفكرية وحقوق المؤلف والحقوق المجاورة والسطو على العلامات الإلكترونية.

الفصل الأول: الجرائم الواقعة على المواقع الإلكترونية، تناولنا فيه جريمة الدخول والبقاء غير المشروع على مواقع التجارة الإلكترونية، و جريمة إتلاف وتدمير المواقع الإلكترونية، وجريمة التزوير المعلوماتي.

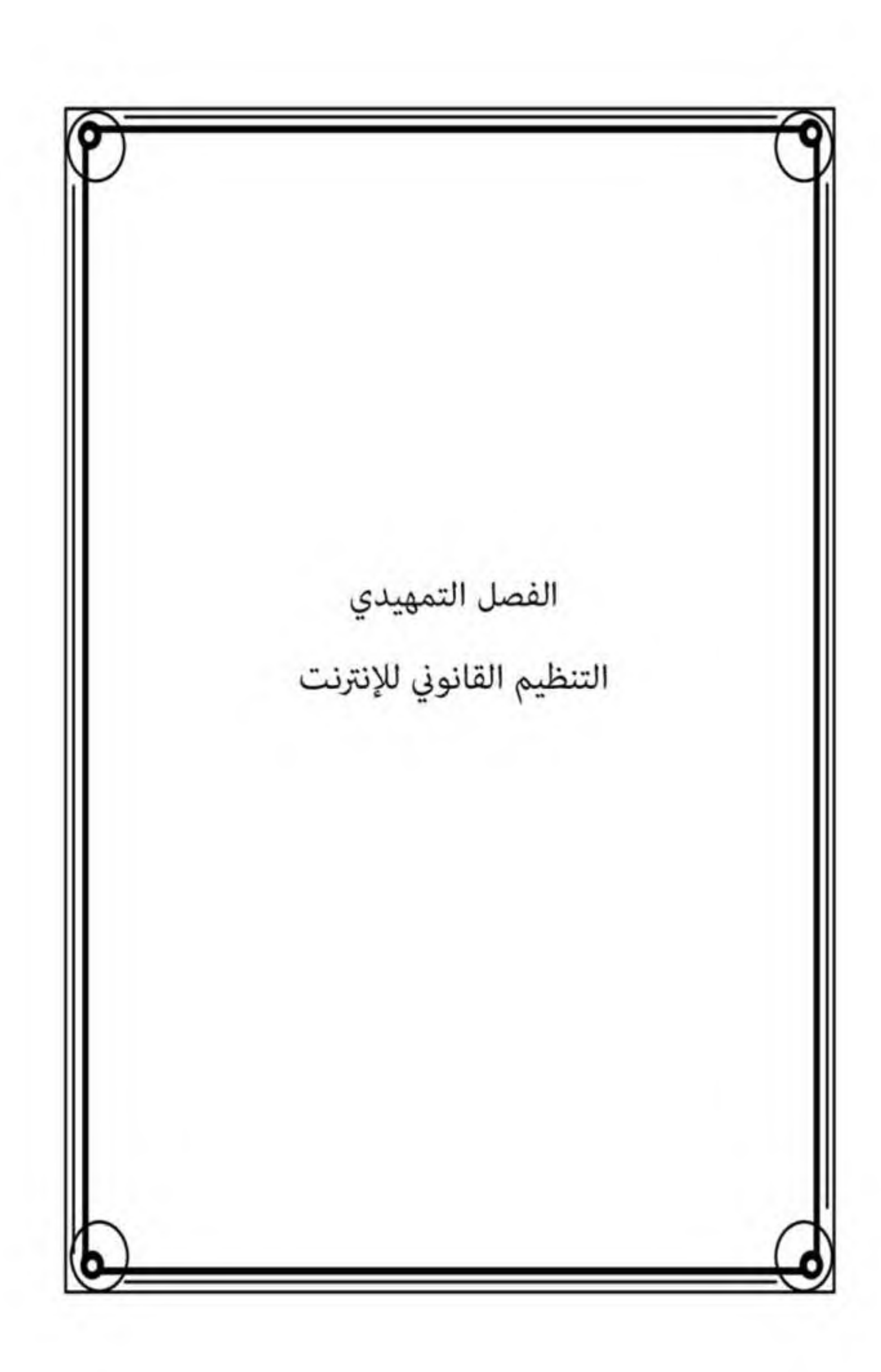
الفصل الثاني: الجرائم الواقعة على البيانات، فتناولنا جريمة التعامل بالبيانات بدون ترخيص، وجريمة انتهاك سرية وخصوصية البيانات، وجريمة التصريح ببيانات غير صحيحة، وجريمة التلاعب في بيانات نظم المعلومات، وأخيرًا الاعتداء على نطاق أسماء الدومين.

الفصل الثالث: الجرائم الواقعة على وسائل التجارة الإلكترونية، تناولنا الاعتداء على التوقيع الإلكتروني، وجرائم إساءة استخدام بطاقات الدفع الإلكتروني، والجرائم الماسة بشهادات المصادقة الإلكترونية.

الفصل الرابع: الجرائم الواقعة على الملكية الفكرية والحقوق المجاورة، بحثنا الحماية الجنائية للمصنف الرقمي، و الحماية الجنائية الدولية والوطنية لحقوق مؤلف برامج الحاسب الآلي، و درسنا تقليد العلامات التجارية.

وتوصلنا في نهاية البحث إلى عدد من النتائج والتوصيات.





الفصل التمهيدي

التنظيم القانوني للإنترنت

الفصل التمهيدي

التنظيم القانوني للإنترنت

تمهيد وتقسيم:

أصبحنا في عالم أزالت تقنيات الاتصال الحدود فيه بين الدول، وسادت ثقافة العولمة في مجالات عديدة ومنها الأنشطة الاقتصادية، ووجدت بيئة جديدة أتاحت للمتعاملين وسائل متطورة للإعلان عن السلع والخدمات ومن ثم التعاقد عليها، بل وتنفيذها أحيانا عبر النقل الآلي للبيانات المجسدة للأداء محل الالتزام، وذلك كله دون حاجة للتواجد المادي أو الشخصي في موقع التعاقد أو التنفيذ.[1]

ونظرًا لما تتمتع به هذه التقنيات من سرعة تؤدي إلى توفير في الوقت والتكاليف وفتح آفاق وأسواق دون عناء، فقد وجد فيها التجار مطالبهم بل حلمهم الخيالي، وبدأنا نسمع عن التسوق الإلكتروني والمعارض الافتراضية، الأمر الذي يمكننا من القول بأنه لم يكن للتقدم التقني في النظام المعلوماتي أثر في تغير محل التجارة فقط، بل أيضًا في تغيير الوسائل التي تتحقق بها هذه التجارة[2]، كل ذلك أدى إلى إمكان إبرام الصفقات من خلال شبكة الإنترنت[3]، وهو ما يطلق عليه بصفة عامة مع شيء من التجاوز

(1) د. أحمد شرف الدين، عقود التجارة الإلكترونية (تكوين العقد وإثباته)، دار النهضة العربية، 2000، ص 5.
(2) د. فاروق الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة، 2002، ص 7.
(3) د. ثروت عبد الحميد، التوقيع الإلكتروني، مكتبة الجلاء الجديدة، المنصورة، 2001، ص3.

وعلى سبيل الشيوع " التجارة الإلكترونية "[1] والتي أصبحت وبحق حقيقة واقعية[2].

وتعتمد التجارة الإلكترونية بشكل رئيسي على شبكة الإنترنت، هذه الشبكة التي أنشئت قبل عقدين، احدثت ثورة في الحياة اليومية للملايين عبر العالم, والتي يرى مبتكروها أنها ما زالت في بدايتها.[3]

هذه الشبكة المؤلفة من ملايين محطات الكمبيوتر المتصلة بالهاتف، والتي أتاحت للبشرية إمكانيات هائلة في مجالات متعددة كالتسويق والدعاية والإعلان والاتصالات والتبادل التجاري والثقافي بين أطرافها مهما بعدت المسافات وتعددت العوائق، وبالتالي يمكن إبرام التعاقدات الإلكترونية بين الأطراف، وأصبح من الممكن لأي منشأة تجارية مهما كان حجمها صغيراً أن تتحول إلى منشأة عالمية بمجرد أن تنشئ لنفسها موقعًا على شبكة الإنترنت[4] حيث يستطيع العالم بأسره التعرف عليها.

وفي خلال فترة زمنية وجيزة وصلت سرعة انتشار شبكة الإنترنت إلى

---

(1) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، دار الكتب القانونية، 2002، ص 9.

(2) د. أحمد شرف الدين، عقود التجارة الإلكترونية، مرجع سابق، ص 6.

(3) حسبما يرى مبتكروها الرئيسيون الذين اجتمعوا في مدريد, ابريل 2009, في مؤتمر "انترناشونال وورلد ويب" الثامن عشر، أن الشبكة تواصل تطورها بالرغم من ظهور تحديات جديدة في مجال الانترنت، من بينها امكان الوصول الى الشبكة في دول العالم الثالث وتطوير تطبيقاته في قطاع الهواتف الخليوية فضلا عن احتمالات نموه الهائلة.
http://www.elaph.com/Web/Technology/2009/4/433295.htm

(4) Catherine L. Mann & Sue E. Eckert، Global Electronic Commerce، Institute for international Economic، A policy Primer، Washington Dc، 2000، p9.

خمسين مليون مستخدم وذلك في أربعة أعوام فقط نظرًا للانخفاض الكبير في أسعار المنتجات الخاصة بتكنولوجيا المعلومات (الكمبيوتر)، وسهولة استخدام شبكة الإنترنت وبخاصة بعد أن صممت شركة مايكروسوفت Microsoft نظام التشغيل Windows[1].

وقبل الخوض في الحديث عن التجارة الإلكترونية من حيث أساسياتها ونشأتها والحماية القانونية المقررة لها وصولا إلى تلك الحماية الجنائية التي ننشدها، وجب علينا الحديث عن هذا الأب الشرعي للتجارة الإلكترونية الحديثة، فما كان للتجارة الإلكترونية أن تصل إلى ما هي عليه الآن لولا شبكة المعلومات العالمية (شبكة الإنترنت).

في البداية مثلت شبكة الإنترنت بيئة مفتوحة وغير مملوكة لأحد، مما أتاح للجميع ممارسة أنشطة متنوعة فيها، ولا تستطيع أي دولة (ولا أي

(1) Jean Camp، Trust and Risk in internet Commerce، the MIT press، Cambridge، England، 2000 p 4.

جاء في تقرير الأمين العام للأمم المتحدة (السيد كوفي عنان) لسنة 2000 ما يلي: (لقد استغرق وصول المذياع إلى 50 مليون شخص 38 عامًا، والتلفزيون 13 عامًا، أما الإنترنت فقد أصبح يستخدمه عدد مماثل من الناس في غضون أربع سنوات فقط، وفي عام 1993 كانت هناك 50 صفحة على الشبكة العالمية، أما اليوم فهناك ما يزيد على 50 مليون صفحة، وفي عام 1998 كان عدد الموصولين بشبكة الإنترنت 143 مليون شخص فقط، ولكن بحلول عام 2001 ارتفع هذا العدد إلى 700 مليون شخص، وفي عام 1996 بلغت معاملات سوق التجارة الإلكترونية 2.6 بليون دولار، وبحلول عام 2002 من المتوقع أن يكون قد وصل إلى 300 بليون دولار، وأصبح للإنترنت بالفعل نطاق من التطبيقات يفوق في اتساعه أي وسيلة أخرى سبق اختراعها من وسائل الاتصال).

د. عمر محمد بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، موسوعة التشريعات العربية، 2003، ص 72.

شخص) ادعاء أنها ابتكرت شبكة الإنترنت، والأرجح أنها تُمثّل سلسلة من الاختراعات المختلفة، انطلقت منذ أن اخترع مورس التلغراف وشفرته، وألكسندر غراهام بل الهاتف، وأديسون المصباح الكهربائي، وماركوني الراديو وغيرها[1].

وفي الوقت نفسه يمكن الحديث عن إسهامات أساسية في صناعة شبكة الإنترنت، سطرتها مجموعة كبيرة من علماء الرياضيات اللامعين (ينتمون إلى دول وعصور مختلفة) ابتدأت مع اكتشاف لايبزينغ للغة الرقمية في القرن الثامن عشر وجورج بوول مؤشرات اللغة الرقمية، وتشارلز بابيج آلة تحليل الحسابات، وتواصلت مع كلود شانون وفون نيومان وغيرهم.[2]

---

(1) صامويل مورس (1791،1872)، مخترع أمريكي يرجع له الفضل في اختراع التلغراف، وصنع أول نموذج عملي للتلغراف سنة 1835 فأحدث ثورة في مجال الاتصالات.

"http://ar.wikipedia.org/wiki/

ألكسندر جراهام بل (1847: 1922م) مخترع اسكتلندي اخترع التليفون.

http://forum.stop55.com/86370.html

توماس ألفا أديسون (1847، 1931م) مخترع أمريكي سجل أديسون باسمه أكثر من ألف اختراع وهو عدد لا يصدقه عقل، مات في نيوجيرسي سنة 1931م.http://ar.wikipedia.org/wiki

غولييلمو ماركوني، ولد في سنة 1874م في إيطاليا، ظل يطور أبحاثه ودراساته حتى توصل أخيرًا إلى اختراع الراديو، وظل يطور ويحسن في اختراعه، وفي سنة 1901م تمكن من إرسال الموجات عبر المحيط الأطلنطي، توفي ماركوني في سنة 1937م.

http://www.arabelect.net/stories/149.htm

(2) لايبزينغ مخترع يرجع له الفضل في اختراع اللغة الرقمية في القرن الثامن عشر.

جورج بول (2 نوفمبر 1815 - 8 ديسمبر 1864) هو عبقري بريطاني ابتكر نوعا من الجبر يتيح التعامل مع الحروف والأشياء والعبارات والفرضيات كما لو=

والأرجح أن شبكة الإنترنت بهذا المعنى تمثل إنجازا إنسانيًا كبيرًا، ويصعب نسبته إلى جهد من جهة محددة بعينها.

وشبكة الإنترنت عبارة عن هيكلية عامة لتبادل الملفات الرقمية، وقد صُممت أنظمة شبكاتها المبنية في شكل يخدم الجميع بشكل عادل متساو، وأراد لها أساتذتها الأوائل (مثل جيروم سالتزر وديفيد كلارك وديفيد ريد وجون بوستل) أن تنقل المعلومات والبيانات بشكل لا يميز بين الأشخاص الذين يقومون بإرسالها، ولا بين أنواع المعلومات المتدفقة عبر فضائها، ولا

= كانت أرقامًا بحتة، وقدم للبشرية الجبر المنطقي المستخدم في الحواسيب والبرمجة. http://ar.wikipedia.org/wiki

تشارلز بباج (26 ديسمبر 1791، 18 أكتوبر 1871) عالم رياضي وفيلسوف ومخترع ومهندس ميكانيكي بريطاني، والذي بدأ مفهوم الحاسوب القابل للبرمجة، درس في جامعة كمبردج وصمم أول حاسبة وأسماها مكنة الفروق (difference engine). وعلى الرغم من أنها لم تستخدم إلا أن فكرتها كانت أساس اختراع الحاسوب، نال منحة من الحكومة من أجل تطوير تصميمه، وقد أنفق تلك المنحة مع جزء من ثروته، ونجح في اختراع آلة أفضل تضارع الحاسبات الحديثة، لكنه توفي دون إكمال آلتيه، ويعتبر بباج بمثابة مخترع الحاسوب الميكانيكي.

كلود إيلود شانون عالم أمريكي في الرياضيات يعتبر من مؤسسي نظرية المعلومات (information theory).

جون فون نيومان (28 ديسمبر 1903، 8 فبراير 1957) هو رياضي أمريكي هنغاري المولد، له إسهامات مهمة في علم الحاسوب والفيزياء الكمية والاقتصاد، وضع معمارية للحساب بالحواسب الرقمية، وقوامها ستة عناصر أساسية تؤمِّن له أداءً متعدد الأغراض، هذه العناصر هي وحدة الحساب، ووحدة المنطق، ووحدة التحكم، ووحدة الذاكرة، ووحدة الإدخال، ووحدة الإخراج، كما رأى أن يعمل الحاسوب باللغة الثنائية، وجميع الحواسيب المستخدمة حاليا تعمل وفق هذا التصميم. http://ar.wikipedia.org/wiki

بين من يتلقونها.[1]

وسوف نتناول هذا الفصل من خلال مبحثين، نبين ماهية شبكة الإنترنت ونشـأتها وأقسـامها وخصائصها في مبحث أول، ونبين قانون الإنترنت في مبحث ثان.

المبحث الأول: شبكة الإنترنت المفهوم – النشأة – الأقسام - الخصائص

المبحث الثاني: قانون الإنترنت



(1) http://www.arab.elaw.com.

المبحث الأول

شبكة الإنترنت

المفهوم - النشأة - الأقسام - الخصائص

انقسم الفقه القانوني في إيجاد تعريف محدد للإنترنت، والمتفق عليه عمومًا هو أن شبكة الإنترنت ظاهرة إنسانية ذات طبيعة تقنية، فهي كما يعرفها مخترع شبكة المعلومات الدولية (تيم برنرز لي[1] Tem Berners

---

(1) السير تيموثي جون برنرز لي "Lee،Berners Timothy John" ولد تيم في الثامن من يونيو 1955، وهو مخترع شبكة الإنترنت العالمية، وعالم فيزيائي، ومخترع تقنية الويب. مشار إليه في: http://ar.wikipedia.org/wiki

ظهر السير تيم بيرنرز لي مخترع شبكة الإنترنت في استطلاعات الرأي كأفضل شخصية بريطانية لعام 2004، ولد في العاصمة البريطانية لندن في 1955، وفي1973 بدأ تعليمه الجامعي في جامعة أوكسفورد، وأثناء تلقيه التعليم الجامعي قبض عليه متلبسًا في عملية اختراق كان يقوم بها من خلال أجهزة الجامعة فحرم من استخدام الأجهزة الجامعية 1980, عمل في معامل CERN السويسرية كمستشار للبرامج في 1984، وفي عام 1989 أطلق مشروعه الذي يضم شبكة الإنترنت وأول سيرفر ومتصفح، وفي عام 1991 قام بوضع رمز WWW على شبكة الإنترنت، كما قام بإنشاء أول موقع على الشبكة، وكان هو موقع معاملCERN ، وفي 1994 قام بيرنرز بتأسيس اتحاد شركات شبكة الإنترنت، وأعلن عن مواصفات ومقاييس التعامل مع الشبكة العالمية. راجع حول ذلك:

http://www.losha.net/vb/showthread.php?t=425 .

وقد أعلن في هلسنكي عام 2004 عن فوز مخترع شبكة المعلومات الدولية بجائزة الألفية الأولى للتكنولوجيا التي تقدمها مؤسسة جائزة التكنولوجيا الفنلندية في هلسنكي، وشهدت قاعة ديبولي للمؤتمرات الواقعة بالقرب من جامعة هلسنكي التكنولوجية مراسم إعلان فوز بيرنرز لي بالجائزة والتي تبلغ قيمتها مليون يورو، وجاء في حيثيات اختيار مخترع الشبكة الدولية أنه باختراعه ساهم في ربط البشر=

lee) مبادرة لنقل المعلومات عبر الوسائل الإلكترونية على نطاق واسع بهدف إتاحة الدخول على وثائق ومستندات عالمية في جميع أنحاء العالم". فهي ووفقًا لهذا التعريف تعد مكتبة عالمية، وهي كما يطلق عليها المهندس الأمريكي تيد نيلسون[1] Ted Nelson المستندات الكونية التي يتم تداولها عبر الكون كله دون ارتباط بوسط أو بيئة أو محيط مخصص، وسوف

= عبر أجهزة الكمبيوتر ليصبح العالم قرية صغيرة تتناقل فيها المعلومات بحرية وسرعة، وهو ما أسهم في تحسين حياة البشر بشكل مباشر وهو أحد شروط منح الجائزة، وقال رئيس لجنة الاختيار في تصريحات للصحفيين: إن شبكة المعلومات الدولية ساهمت في حصول البشر على المعلومات المهمة لحياتهم، وبناء أنواع جديدة ومستحدثة من العلاقات الاجتماعية، وإعلاء قيم الديمقراطية والشفافية ودفع الاقتصاد الدولي. قد قام بيرنرز لي أيضا باختراع النظم الخاصة بالتعامل مع شبكة الإنترنت مثل المزود ومعرف المواقع ونظام نقل النصوص، إلى جانب لغة كتابة صفحات شبكة الإنترنت، كما أنه يرجع إلى بيرنرز الفضل في اختراع المتصفح، وهو ما جعل من الشبكة الدولية ساحة لتبادل المعلومات عبر لغة مشتركة يعرفها الجميع، ويعمل بيرنرز الآن باحثا في معهد ماساتشوستس للتكنولوجيا في بوسطن بالولايات المتحدة الأمريكية، وفي العام الماضي حصل على لقب فارس من ملكة إنجلترا نظرا لأعماله المتفردة في مجال تكنولوجيا المعلومات، وجائزة الألفية للتكنولوجيا هي الأولى والأكبر من نوعها، وتقدم لنيلها 78 مخترعا من 22 دولة، وشملت المجالات التي تسابق فيها المخترعون كلا من الصحة والاتصالات والمعلومات والطاقة والبيئة إلى جانب المواد الجديدة وطرق المعالجة المستحدثة لهذه المواد، وتمنح المؤسسة جائزتها الكبرى البالغة مليون يورو مرة كل عامين.

http://www.anageed.com/vb/archive/index.php/t.10008.html

(1) تيد نيلسون: Ted Nelson مهندس اتصالات أمريكي قام بتطوير الخطوط النشطة عام 1965 مما أدى إلى وجود المستندات الكونية Decuvers، وقام بإنشاء مكتب يقوم فعليا بربط أي مستند بمستندات أخرى مشابهة في العنوان أو في أي عنصر من عناصر المحتوى.

نتناول هذا المبحث وفقًا للتقسيم التالي:

المطلب الأول: ماهية شبكة الإنترنت ونشأتها وتطورها

المطلب الثاني: تعريف شبكة الإنترنت

المطلب الثالث: أقسام شبكة الإنترنت

المطلب الرابع: خصائص شبكة الإنترنت



المطلب الأول

ماهية شبكة الإنترنت ونشأتها وتطورها

يتكون اصطلاح شبكة الإنترنت من اختصار كلمتين International وNetwork ويقصد بها شبكة الاتصالات الدولية، وهي شبكة هائلة من أجهزة الكمبيوتر المتصلة فيما بينها بواسطة خطوط الاتصال عبر العالم، سواء أكانت مسموعة أم مرئية، وهي شبكة دولية تعمل بفضل البنية التحتية للاتصالات عن بُعد[1]، وأتاحت إنجاز الخدمات التجارية من خلال مواقع الويب(web)، ونتناول هذا المطلب من خلال فرعين: الأول ماهية شبكة الإنترنت، والثاني نشأتها وتطورها.

الفرع الأول

ماهية شبكة الإنترنت

من أهم التعريفات التي قيلت عن شبكة الإنترنت أنها " شبكة هائلة من أجهزة الكمبيوتر المتصلة فيما بينها بواسطة خطوط الاتصال عبر العالم[2]"

ويعرف البعض شبكة الإنترنت بالنظر إلى الخدمات المتاحة " بأنها من وسائل الاتصال المسموعة والمرئية في آن واحد[3] " ويرون أنها من وسائل

(1) د. أسامه أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص5.

(2) شبكة الإنترنت تعتبر مجموعة شبكات وأجهزة الحاسب الإلكتروني التي توجد في مختلف دول العالم والتي تتصل ببعضها ويجمع بينها أنظمة الاتصالات الإلكترونية التي تستخدم لنقل البيانات Transmission Control Protocol/ Internet Protocol TCP/IP، أي نظام نقل المعلومات.

Roger Leroy Miller & Gaylord A.Jentz، Law for Electronic Commerce Thomson Learning، 2000،p4.

(3) د. فاروق الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، =

الاتصال عن بُعد، ذلك لأنها شبكة دولية تعمل بفضل البنية التحتية للاتصالات عن بُعد.

ويمكن تعريف الاتصالات عن بُعد بأنها " كل انتقال إرسال أو استقبال لرموز، أو إشارات، أو كتابة، أو صور، أو أصوات، أو معلومات أيًا كانت طبيعتها بواسطة ألياف بصرية أو كهربائية لاسلكية أو أية أنظمة إلكترومغناطيسية أخرى"[1].

وتمثل شبكة الإنترنت وفقا للتعريفين السابقين نظامًا هائلا من شبكات الكمبيوتر المتصلة ببعضها البعض الممتدة عبر العالم، وباستخدام شبكة الإنترنت يمكننا التواصل مع أناس آخرين عبر العالم بواسطة البريد الإلكتروني والقراءة الفورية لنسخ الصحف والمجلات والجرائد الأكاديمية والكتب، والمشاركة في مجموعات المناقشات حول أي موضوع، والمشاركة في الألعاب والمحاكاة، وفي السنوات الأخيرة أتاحت شبكة الإنترنت الخدمات التجارية من خلال مواقع الويب (web)، وأمكن لأي شخص لديه كمبيوتر شخصي pc مزود بجهاز المودم Modem[2] ولديه اشتراك لدى أحد مقدمي خدمة شبكة الإنترنت وخط تليفون الدخول على شبكة الإنترنت والاستفادة من الخدمات المتاحة عليها.

= مرجع سابق، ص 8.

(1) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص5.

(2) المودم Modem اختصار لكلمتين Modulator demodulator وهو جهاز يسمح بنقل البيانات إرسالا واستقبالا بين الكمبيوتر والأطراف الإعلامية من خلال الأسلاك التليفونية.

الفرع الثاني

نشأة شبكة الإنترنت وتطورها

ترجع جذور التقنيات الموجودة على شبكة الإنترنت إلى عام 1957، وكان وقتًا عصيبًا بين الولايات المتحدة والاتحاد السوفيتي السابق حيث كانت " الحرب الباردة " بين البلدين في ذروتها، ففي الرابع من تشرين أول (أكتوبر) عام 1957، فاز الاتحاد السوفيتي بالرهان من خلال إطلاق مركبة " سبوتنيك1 " وهي أول قمر صناعي يدور حول الأرض، وكان لهذا النجاح أثره البالغ على الولايات المتحدة الأمريكية التي قررت إنشاء " هيئة المشروعات والبحوث المتطورة " التابعة لوزارة الدفاع الأمريكية (البنتاجون)، والتي تعرف اختصارًا بـ ARPA [1] بهدف تطوير تقنيات خاصة للجيش الأمريكي تمكنه من التقدم على السوفييت، وكانت الغاية أن تصبح هيئة المشروعات هي الجهة المسئولة عن تطوير الجيش الأمريكي، وقامت الهيئة بتوظيف العديد من الباحثين والعلماء في مشروعات مختلفة في مجالي الدفاع والبحوث[2].

وقد بدأت شبكة الإنترنت حياتها في الستينيات من القرن الماضي وبالتحديد عام 1962[3] على يد مجموعة مهرة من علماء التقنية العاملين في وكالة الأبحاث والمشروعات المتطورة.

(1) هيئة المشاريع والبحوث المتطورة (The Advanced Research Project Agency).

(2) Warwick Ford & Michael S. Baum، Secure Electronic Commerce Building the Infrastructure for Digital Signatures and Encryption، prentice Hall، 'New Jersy 2001 p 17

(3) Clive Gringras،The laws of the internet، Butter worth's press London 1997 p2

وفي عام 1964 تولت هذه الوكالة ARPA إيجاد أفضل طريقة للاتصال بعدد غير محدود من أجهزة الكمبيوتر[1] دون اعتماد على جهاز كمبيوتر واحد ينظم حركة السير[2]، وذلك من أجل الحفاظ على نظام اتصالات آمن في حالة حدوث كارثة سواء أكانت طبيعية كالزلزال أم من صنع الإنسان كهجوم ذري أو نووي أو نشوب حرب غير تقليدية[3]، ولذلك عمل البنتاجون على البحث عن تكنولوجيا جديدة للاتصالات، فقام بتمويل وإعداد شبكة تعد من أهم شبكات الكمبيوتر.

وفي عام 1968 تم اجتياز أول تجارب الشركة في معمل الأبحاث الوطنية في بريطانيا، وفي عام 1969 قامت ARPA باستعمال هذه الشبكة رسميًا وذلك بتصميم برنامج للتمكن من تشغيل الحاسوب من قبل عسكريين ومسئولين بشئون الدفاع، وفي عام 1973 بدأت الاتصالات الدولية بشبكة ARPA NET من إنجلترا والنرويج، ويمكن القول أن البداية الحقيقية للإنترنت كانت في هذا العام.

ازداد اتساع شبكة الإنترنت حتى انفصلت الشبكة العسكرية عن الشبكة الأم عام 1983.

وفي عام 1986 تم نقل تشغيل ARPA NET من إدارة الدفاع إلى

(1) وقد استعملت عدة مصطلحات في اللغة العربية للدلالة على كلمة كمبيوتر مثل الحاسوب أو الحاسب الآلي أو الحاسب الإلكتروني، ويسمى بالفرنسية Ordinateur ولمزيد من التفاصيل راجع د. محمد حسام لطفي، الحماية القانونية لبرنامج الحاسب الآلي، دار الثقافة العربية، 1987، ص 5.

(2) د. محمد السعيد رشدي، شبكة الإنترنت والجوانب القانونية لنظم المعلومات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، الكويت، 1997، ص11.

(3) Horgan Sarch B. to net or not to net، federal Communication Law Journal "USA" vol 51 no 2 1999 p 431.

شبكة مؤسسة العلوم الوطنية، ثم تطور مشروع (ARPA) تدريجيا حتى تحقق لهذه الشبكة[1] الانطلاق والتوسع عندما تبنتها شبكة مؤسسة العلوم الوطنية National (NSF) Science Foundation وذلك بهدف السماح باطلاع المجتمع العلمي على كافة المعلومات المخزنة على الشبكة وأصبح اسمها المختصر NSFNET[2].

وفي عام 1990 انتهت ARPAnet لتتحول إلى شبكة الإنترنت، وذلك بترابط خمس شبكات هي ARPAnet،USEnet ،BITnet، CSN،NSFnet ولم يقف الأمر عند هذا الحد، بل وبسرعة فائقة انضمت شبكات أخرى عديدة منها ما هو محلي ومنها ما هو دولي، كالشبكات التي تنتمي للدول التي ترتبط مع الولايات المتحدة باتفاقيات خاصة حول الاتصالات، وفي العام ذاته بدأ ظهور خدمة البريد الإلكتروني، وتقديم معلومات عن أسعار البورصات العالمية وأسعار سوق المال، وبيانات ومعلومات عن أعمال البنوك، ومن هنا أصبحت شبكة الإنترنت تستخدم في أغراض أخرى غير الأغراض العلمية، وتزايدت الاتصالات الإلكترونية من خلالها، إلى أن صارت تستخدم في الأغراض التجارية بعد أن كانت حكرًا على مجموعة من العلماء والباحثين.

وفي عام 1991 تمكن مهندس الاتصالات الإنجليزي تيم بريترز لي Tem Berners lee[3] من اختراع شبكة المعلومات الدولية WORLD WILD WEB أو المعروفة اختصارًا بـ WWW، وفي ذات العام تم

(1) J. Dianne Brinson، Analyzing E. Commerce & Internet Law، prentice hall PTR، New Jersey، USA، 2001،p7.

(2) L. Jean Camp, Trust & Risk in Internet Commerce, MIT Press, Winter (Cambridge, MA) 2000 p 6،7.

(3) سابق الإشارة إليه.

إطلاق الشبكة المذكورة من المعمل الأوروبي للفيزياء الذرية في سيرن CERN بسويسرا[1].

ولقد ازداد عدد مواقع الانترنت على نحو متسارع ليبلغ حاليا ثمانين مليونا، في حين كان بالكاد 500 في العام 1994. ورافق هذه الزيادة نمو لافت للمدونات الالكترونية المواقع الشخصية التي يتولى افراد يستخدمون الشبكة الالكترونية تزويدها بالمعلومات.[2]

وفي عام 1992 أعلن الرئيس الأمريكي بيل كلينتون أثناء حملته الانتخابية عن الطرق السريعة للمعلومات، ويقصد بهذا المفهوم الجديد تطوير البنية التحتية الأرضية والفضائية لشبكات الاتصالات الوطنية باتجاه بناء السوبر أو أوتوستراد المعلومات العابر للقارات،[3] باستخدام أنظمة الترقيم والوسائط المتعددة والألياف البصرية والضوئية القادرة على

---

(1) لقد تكونت هذه الشبكة من مراكز لخطوط الإرسال، وبمساعدة الاتصالات عبر الأقمار الصناعية والموجات الدقيقة أمكنها أن تحمل كميات هائلة من المعلومات التي تتحرك لمسافات بعيدة بسرعة هائلة.
وأضحت هذه الشبكة هي المكون الأساسي للبنية التحتية للإنترنت، وخاصة بعد أن رفعت الحكومة الأمريكية يدها عنها وبدأت تقديم خدمة شبكة الإنترنت للناس عمليا.

(2) http://www.elaph.com/Web/Technology/2009/4/433295.htm

(3) ويسمى (Electronic super high ways) أو ((Auto Route،Super ولم يظهر سوى ملامح بسيطة لهذا الحدث المنتظر حيث كثر الحديث عنه مؤخرًا أنه يوفر أقوى الوسائل للدفع الآمن عبر الشبكة، ويحقق مستوى أفضل من المجلس الافتراضي وعمليات التعامل عن بعد، ويشاع أن تطبيقاته المرتقبة تأتي ضمن ما يسمى بالحكومات الإلكترونية أو الإدارة الإلكترونية. راجع د. خالد إبراهيم ممدوح، إبرام العقد الإلكتروني، رسالة دكتوراه، جامعة الإسكندرية، 2005، ص14.

استيعاب وتدفق المعلومات والبيانات الهائلة عبر شبكات الاتصالات عن بُعد، التي تتفوق بقوة على الشبكات الهاتفية التقليدية[1].

ولقد نشأ عن استخدام شبكة الإنترنت تكوين ما يسمى بعالم الفضاء الافتراضي أو الخيالي أو Cyber Space أو الفضاء المصطنع الإلكتروني[2]، حيث يتم تبادل المعلومات والبيانات في هذا الفضاء بطريقة إلكترونية، ومما لا شك فيه أن مصطلح الفضاء الإلكتروني من المصطلحات الجديدة على قواميس اللغة العربية ولكن ذلك له ما يبرره؛ حيث إنها لم تظهر في القواميس الغربية إلا في السنوات الأخيرة فقط[3]، وقد أدى ظهور عالم الفضاء الافتراضي إلى ظهور نظام تبادل البيانات إلكترونيًا والذي أصبح حقيقة واقعية تفرض نفسها خاصة في مجال التجارة الإلكترونية[4] التي انتشرت بسرعة مذهلة بين دول العالم كافة.[5]

---

(1) Ejan Mackaay & Daniel Poulin، The Electronic Super Highway، The shape of Technology and Law to come Kluwer Law International 1995، p37.

(2) د. محمد السعيد رشدي، شبكة الإنترنت والجوانب القانونية لنظم المعلومات، المرجع السابق، ص 11.

(3) وهناك مصطلحات كثيرة وجديدة على قواميس اللغة العربية وهي نتاج ثورة المعلومات، ومن هذه المعلومات الواقع الافتراضي Virtual Reality والبريد الإلكتروني E -mail والنص المتشعب Hyper Text وقانون الفضاء الإلكتروني Cyber Law والفضاء الإلكتروني Cyber Space.

(4) فريد هـ كيت، الخصوصية في عصر المعلومات، ترجمة محمد محمود شهاب، بدون ناشر، 2000، ص 9.

(5) www.albawaba.com/ar/literature,lterary_lnalysis/276136

المطلب الثاني

تعريف شبكة الإنترنت

انتشار شبكة الإنترنت حمل معه تيارين مختلفين من الحماس والقلق، الحماس من أجل فتح باب جديد لحرية الاتصال بأشخاص لا يمكن الاتصال بهم في الواقع بسهولة، وإمكانية عقد صفات تجارية عن بعد، أما القلق فمن أجل احتمال عدم تأمين الاتصالات أو انتهاك السرية عبر شبكة الإنترنت، أو القيام بأعمال القرصنة، أو انتهاك حق الخصوصية The Right of Privacy، والاطلاع على البيانات الشخصية وحسابات البنوك، أو استخدامها في تجارة مشبوهة كالمخدرات وتجارة السلاح وعمليات بيع الأطفال، وأيضًا استخدام شبكة الإنترنت في النشاط التخابري والإضرار بأمن الدولة.

وفي الوقت نفسه يسهل عبر الشبكات الإلكترونية الوصول إلى معلومات سرية قد تتصل اتصالا وثيقًا بخصوصية الإنسان، وهو أمر بالطبع يثير القلق والحيرة، ويزيد من حدته أن هذه المعلومات إذا ما تم تجميعها والربط بينها واستكمالها يمكن أن تظهر جوانب يضر كشفها وظهورها بمصالح بعض الأفراد، بل وبأمن واستقرار الدولة نفسها.

والتجارة الإلكترونية ليست بمأمن من كل هذه الأخطار على اعتبار أنها تعتمد في نشاطها على التقنية، والتي تعتبر عصب حياة هذه التجارة، وشبكة الإنترنت كانت منذ سنوات قليلة تستخدم لتبادل البيانات والمعلومات أو التعليم، وأصبحت الآن معبرًا أساسيًا للتجارة الدولية بين الدول.

ومن ناحية أخرى فقد أدى ظهور شبكة الإنترنت إلى انتشار وازدهار مجالات كثيرة لم يكن لها أن تنتشر لولا وجودها، منها تزايد النمو في

مجال التمويل الإلكتروني للبنوك E-Finance حيث يتضمن جميع أنشطة التمويل التي يمكن تنفيذها من خلال شبكة الإنترنت أو الشبكات العامة، مثل شبكات الربط الفوري بين مجموعة من البنوك، كما ساعدت على انتشار المنتجات والخدمات المالية مثل التأمين وخدمات الرهن العقاري Mortgage، والسمسرة والنقود الرقمية Digital Money والدفع الإلكتروني.

وسنتناول في هذا المطلب تعريف شبكة الإنترنت باعتبارها وسيلة تواصلية بين الشبكات دون اعتبار للحدود الدولية، ونحدد عناصرها وما تستلزمه فكرة أن شبكة الإنترنت وسيلة تواصلية من ضرورة توافر المعلومات دون اعتبار للحدود، ثم نتبع ذلك ببيان لعناصر التعريف.

أولا: تعريف شبكة الإنترنت:

تعرف شبكة الإنترنت International Network/ Internet " بأنها الوسيلة أو الأداة التواصلية بين الشبكات دون اعتبار للحدود الدولية".[1]

ومن هذا التعريف نقف لا على طبيعة شبكة الإنترنت وإنما على حقيقتها، إذ إنها من طبيعة تقنية - إنسانية، بمعنى أنها نتاج اجتماع التقنية والمعلوماتية، ثم إنها وسيلة تواصل بين الشبكات، والاتصال الذي يحدثه شبكة الإنترنت هو مجرد إحداث عملية تماس بين شبكة فأكثر، أو عملية

(1) كما يدل اسمها وما سبق وأن أشرنا إليه، فإن شبكة الإنترنت هي شبكة ما بين عدة شبكات تدار كل منها بمعزل عن الأخرى بشكل غير مركزي، ولا تعتمد أي منها في تشغيلها على الأخريات، كما قد تستخدم في كل منها داخليا تقنيات حاسوبية وشبكية مختلفة، وما يجمع بينها هو أن هذه الشبكات تتصل فيما بينها عن طريق بوابات تربطها ببروتوكول مشترك قياسي هو بروتوكول إنترنت. http://ar.wikipedia.org/wiki

انتقال من حيث يكون ملقم المستخدم إلى شبكة أخرى أينما كانت، وعليه فشبكة الإنترنت في الحقيقة كأداة تواصلية ينتهي دورها بمجرد الدخول إلى شبكة الغير.

ثانيًا: عناصر التعريف:

القول بأن شبكة الإنترنت (هي تلك الوسيلة أو الأداة التواصلية بين الشبكات المعلوماتية دون اعتبار للحدود الدولية) يجعلنا بالتأكيد نأخذ بالاتجاه التقني - الإنساني في تعريف شبكة الإنترنت، فهو الاتجاه الذي يضع النظام المعلوماتي كعنصر جوهري في شبكة الإنترنت[1]، وفي الوقت ذاته يأخذ في الاعتبار دور التقنية باعتبارها مخرج شبكة الإنترنت إلى الوجود.

أ - شبكة الإنترنت وسيلة تواصلية:

شبكة الإنترنت وسيلة تواصلية تعتمد على التقنية، إذ إن عددًا من أجهزة الحاسوب المتصلة ببعضها البعض تخلق نظامًا System اتصاليًا، وعدة أنظمة متصلة ببعضها تخلق شبكة، وعدة آلاف من الشبكات منطلقة من المحلية إلى العالمية متصلة بشكل عنكبوتي ببروتوكول اتصالي انفتاحي (T C P / I P) هو المنظم للاتصال بين أجهزة الحاسوب عبر شبكة الإنترنت نكون عن طريقها قد وصلنا إلى نقطة اللامركزية، وبالتالي يتم التواصل بين هذه الشبكات والأجهزة، وهذا كله تعبير عن التواصل بين الشبكات بحيث يبرز الدور الاتصالي الذي تقوم به التقنية تعبيرًا عن تلك الوسيلة.

---

(1) L. Jean Camp، Peer to Peer Systems، The Internet Encyclopedia ed. Hossein Bidgoli, John Wiley & Sons (Hoboken, New Jersey) 2003، p 5.

ب - شبكة الإنترنت تستلزم المعلومات:

إذ إنه بدون النظام المعلوماتي التبادلي بين الشبكات فإن شبكة الإنترنت تصبح منهجًا بدون موضوع، حتى بافتراض التخصص والسرية والتشفير وهو أمر موجود حاليًا، فإن شبكة الإنترنت كانت قد خلقت نظامًا تواصليًا بين الشبكات هدفه تبادل المعلومات، فليس للتقنية قيمة في ذاتها وإنما هي وسيلة إلى تنظيم العمل بموضوع ما والاستفادة منه، فهي كالفلسفة منهج بدون موضوع، فإذا أضفنا المعلومات كموضوع للتقنية فإننا نكون بصدد شبكة الإنترنت. ولأجل ذلك فإن المعلومة Information ذات أهمية قصوى في إطار عمل الشبكة، فهي سيدة الموقف عبر شبكة الإنترنت.

والمعلومة تحتاج إلى الإنسان لكي يضعها، والإنسان بحاجة إلى دعم مادي ومعنوي في حمايته لهذه المعلومة، ويصل هذا الدعم في بعض الأحيان إلى ضرورة التدخل، ليس الحكومي فقط في إطار دولته، وإنما إلى الدعم ذي البعد الدولي على عمومه أيضًا، ومن الضروري القيام في إطار التعاون الدولي بعقد اتفاقيات وتجديد تلك الاتفاقيات النافذة لحماية نظم المعلومات عبر شبكة الإنترنت[1].

ومن أهم مظاهر الحماية الواردة على النظام المعلوماتي عبر شبكة الإنترنت تلك الدعوة التي برزت في مقدمة عمل البيت الأبيض الأمريكي حول التجارة الإلكترونية White house paper on electronic commerce الصادرة في 30 / 6 / 1997، وكذلك إعلان بون Bonn

(1) د. شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، مرجع سابق، ص 13، وفي المعنى ذاته: د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004، ص 32.

Declaration الصـادر في 24 / 11 / 1997 حـول الإدارة الذاتيـة أو التنظـيم الـذاتي للعـالم الافتراضي Cyber self - government عبر شبكة الإنترنت بقصد التعرف الـذاتي عـلى الأحكـام واستخلاص النظم، وهي دعوة يوجد لها أساس تاريخي، فقد نادى بها منذ أكثر مـن نصـف قـرن الأستاذ الإيطالي جوجيو ديلفيكيو أستاذ فلسفة القانون ومدير جامعة روما الذي وإن كـان يؤيـد قاعدة أن الدولة هي صاحبة الصفة الوضعية للقـانون إلا أنـه مـع ذلـك لم يمـانع مـن التصريـح بقبول الأنظمة القانونية التي تبتكرها المنظمات الخاصة في إطار الدولة ما دامت تعمـل في إطـار النظام الوضـعي القـائم، فكـان البروفيسـور ديلفيكيـو مـن أوائـل الـذين قـاموا بطـرح موضـوع الحوكمة Governance وهو من الموضوعات التي تأثرت بها فلسفة هيكلة المجتمع المعلومـاتي القائم[1].

ج - شبكة الإنترنت تتجاوز الحدود الوطنية:

يثير هذا العنصر الثالث من عناصر التعريف الكثير من الجدل حول شبكة الإنترنـت، حيـث إن شبكة الإنترنت ليس لها حدود دولية، ولا تعترف بتلك الحـدود القائمـة بـين الـدول، كـما أنهـا ليست مملوكة لأحد، وبالتالي فليس هناك جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها، وهذا يعني أنه يمكننا الدخول إلى شبكات الغير، كما أن الغير يسـتطيع الـدخول إلى الشـبكات الخاصـة بنا، وكذلك إلى حواسيبنا.

ظاهرة شبكة الإنترنت العلمية ليست سوى ظاهرة دولية تنعدم مركزيتها فتتسـاوى أمامهـا الدول الكبيرة والصغيرة، دون المساس بسيادة هذه الدول.

(1) جوجيو ديلفيكيو مقال بعنوان: فلسفة القانون في إيجاز، ترجمة د. ثروت أنيس الأسيوطي، منشـور بمجلـة القانون والاقتصاد، الصادرة عن كلية الحقوق جامعة القاهرة، السنة 12 / 1972، العدد الأول، ص 755.

لأن الأمر الحاكم في شبكة الإنترنت هو القدرة المعلوماتية، وسوف يأتي الوقت الذي يكون فيه الأكثر تميزًا من يملك هذه القدرة المعلوماتية، والتي تشكل قواعد بيانات محملة على شبكة الإنترنت، وهو ما يعني كذلك ظهور مستويات اجتماعية واقتصادية مختلفة عن تلك المستويات الناتجة عن الثروة، نظرًا لأن شبكة الإنترنت هي ذاتها تمثل ثورة علمية لنشر المعرفة وتداول البيانات دون رقابة ودون فواصل بين الشعوب متجاوزة في ذلك الحدود الوطنية.

وقد ساعد على ذلك - رغم حداثة العمر - التقنية العالية في وسائل الاتصال والعولمة الاقتصادية، وظهور التجارة الإلكترونية، والحاجة لبث المعلومات والاعتماد عليها في اتخاذ القرار في شتى المجالات السياسية والاقتصادية والاجتماعية، ومع ذلك فإن الدول الصغيرة ذات الإمكانيات التقنية الضعيفة - وهي دول سوف تجد نفسها بحاجة إلى شبكة الإنترنت إزاء التطور البشري الهائل في استخداماتها - يمكن أن تصادف مسألة حجب التقنية خصوصًا في مثل هذه النوعية التي تهيمن عليها دول مثل الولايات المتحدة الأمريكية والمملكة المتحدة، خصوصًا في مسائل تقنيات الحاسوب.[1]

(1) نعتقد أن هذا الأمر امتد حتما إلى تقنيات الحاسوب كنوع من فرض الهيمنة المقصودة ليس على تلك الدول وإنما على شبكة الإنترنت ذاتها، لاسيما وأن دولا مثل الولايات المتحدة وتابعيها كبريطانيا تلجأ إلى مثل هذه النوعية من الهيمنة، فمثلا ظلت تقنية التشفير في إطار الحظر المفروض بقوة القانون الأمريكي لمدة طويلة، كما أن العديد من البرمجيات مثل برمجية مطاردة الهكرة Actis التي أنتجتها شركة ACTIS TECHNOLOGY الإنجليزية رفضت التعامل مع دول مثل سنغافورة والصين بحجة حقوق الإنسان، والأمثلة على ذلك كثيرة ومتعددة تتكرر يوميا أيضا، كما شرعت دول مختلفة من خلال مشرعيها وقوانينها في =

المطلب الثالث

أقسام شبكة الإنترنت

شبكة الإنترنت باعتبارها وسيلة أو أداة تواصلية تنقلنا إلى العالم

= بسط سيطرتها على هذه الوسيلة من وسائل التعبير، فسنت الولايات المتحدة مثلا قوانين عدة للتدخل الحكومي في شبكة الإنترنت، بحجة حماية الملكية الفكرية تارة، أو حماية الملكية الخاصة تارة أخرى، كما أصدرت محاكمها أحكامًا بخصوص شبكة الإنترنت في أكثر من مناسبة، مثلما حدث مثلا في قضية موقع «نابستر» Napster لتبادل الملفات الموسيقية، الذي خضع لحكم أميركي ألزمه بإيقاف ذلك التبادل، كما سنّت «قانون حقوق المؤلف الرقمية في الألفية الجديدة» Digital Millennium Copyright Act، وأيضًا صدرت قوانين أميركية تسمح للسلطات التنفيذية بتعقب حواسيب الأشخاص الذين يعتدون على حقوق الملكية الفكرية، بما في ذلك الملفات الموسيقية ومصادرتها، وحذت كثير من الدول حذو أمريكا، فسنت قوانين جديدة أو شددت قوانين الملكية الفكرية فيها، ويرى البعض أن من شأن تلك التوجّهات القانونية أن تحدّ من الحرية الإلكترونية وتزيد من سيطرة الدول على هذه الشبكة بأكثر مما تفعل بالنسبة إلى الوسائل الأخرى، واستخدمت كثير من الدول تقنيات الرقابة الإلكترونية بكثافة لافتة، فحصلت الصين على أجهزة ضخمة تمكنها من منع دخول الصينيين إلى المواقع السياسية، وكذلك تعقب من يتحدى المنع، واستخدمت الحكومة الصينية تقنيات عدة لتنقية filtering رسائل البريد الإلكتروني تتيح استخراج الرسائل التي تتضمن كلامًا سياسيًا، وتحاول بعض الشركات المتخصصة في أنظمة الشبكات مثل شركة «سيسكو سيستمز» أن تميّز الأشخاص الذين يستخدمون شبكة الإنترنت والمواد التي يرسلونها، وطورت موجّهات تسمح لشركات الاتصال بأن تتحكم في سرعة نقل البيانات والمعلومات عبر شبكة الإنترنت دون التدخل في هوية صاحبها، وهكذا يمكن القول بأن الصراع قد انتقل من الطبقة العليا حيث يجري تناقل المحتوى الإلكتروني، إلى «الطبقة المنطقية» حيث تحاول الشركات والدول التحكّم ببروتوكولات شبكة الإنترنت أيضًا، بعد أن ساد الاعتقاد طويلا بحريتها. http://www.arabelaw.com

الافتراضي الذي أوجدته في حياة البشر، حيث يتم تبادل المعلومات والبيانات في هذا الفضاء إلكترونيًا، وقد تطرق الفقه المقارن إلى أقسام شبكة الإنترنت استنادًا إلى الأساس الخدمي للإنترنت، فيأخذ بالتقسيم الثلاثي وهو ما سوف نتناوله باعتباره التقسيم الراجح في الفقه المقارن، وهذه الأقسام هي شبكة المعلومات الدولية، والبريد الإلكتروني، والاتصال المباشر[1].

هذه الأقسام الثلاثة لا تُعد في حقيقة الأمر منتهى الحركة في شبكة الإنترنت، وإنما فقط ما هو موجود حاليًا من أقسام لها، إذ يمكن أن تزيد معدلات حركة الاستخدام لتأتي بقسم جديد أو أكثر فتتزايد هذه الأقسام، ولعل الملاحظ على هذا التقسيم أنه ليس هناك فاصل كلي بين هذه الأقسام، فهي متداخلة فيما بينها، لذلك يصعب ملاحظتها، فيستطيع مستخدم شبكة

(1) يضيف البعض أقساما أخرى للإنترنت، مثل:

بروتوكول نقل الملفات File Transfer Protocol (FTP): والذي يمكن من خلاله نقل أي كمية من الملفات أو البرامج من الكمبيوتر لأي شركة أو مؤسسة أعمال أو غير ذلك ووضعها على ذاكرة جهاز الكمبيوتر الخاص بالجهة الأخرى، وتتميز هذه الطريقة بسهولتها بالمقارنة بعملية نقل الملفات عن طريق الأقراص أو الأشرطة الممغنطة.

وقوائم البريد الإلكترونية Electronic Mailing List: وهي طريقة يمكن استخدامها لتبادل الآراء والنقاش حول موضوع معين بين مجموعة من الأشخاص، وهي أشبه بنظام التخاطب عبر شبكة الإنترنت Internet Relay Chat (IRC).

والتيلنت Telnet: وهو برنامج خاص يستخدم للربط بين كافة أجهزة الكمبيوتر في كافة أنحاء العالم، ويمكّن من استخدام قاعدة البيانات الموجودة في الكمبيوترات الأخرى، وهذه الخدمة تسمى أحيانًا "الارتباط عن بعد" Remote Login، وغالبًا ما يستخدم في العمليات التجارية، ولكن يلاحظ أن هذا النظام بدأ في الاختفاء بسبب تزايد إقبال المستخدمين على شبكة الويب Web لسهولة التعامل معها.

الإنترنت أن يتصفح أو يبحر، وفي الوقت ذاته يرسل رسالة إلكترونية، وكذلك يتحادث مباشرة مع أشخاص في أماكن أخرى، وربما يأتي يوم تتجاوز فيه شبكة الإنترنت المجال الأرضي إلى الكواكب الأخرى التي تدور حول الكرة الأرضية، وهو أمر ليس بعيد الاحتمال إذا استشعرنا مدى القدرة الإيجابية التي تتمتع بها شبكة الإنترنت والمفارقة الحادثة في فكرة الأدب المعلوماتي والخيال العلمي[1]، فبعد أن كان مجرد خيال أصبحت تصوراته ممكنة، وأضحى العقل البشري منشغلا به، وسوف نعرض لهذه الأقسام الثلاث من خلال ثلاثة فروع:

الفرع الأول

شبكة المعلومات الدولية

نتناول في هذا الفرع التعريف بشبكة المعلومات الدولية، مع إعطاء نبذة تاريخية عنها، وأهميتها، وما نجم عنها من مشكلات قانونية.

وهي تعرف اصطلاحًا بـ World Wide Web واختصارًا يرمز لها بالأحرف "WWW" وتعتبر هذه الشبكة من الشبكات الرئيسية الموجودة على شبكة الإنترنت، وتسمى web اختصارًا، والتي يعبر عنها البعض بالعربية بالشبكة العنكبوتية العالمية[2]، ويمكن تعريفها بأنها مجموعة

---

(1) لقد فجرت رواية نيو رومانسر New Romancer أو الحالم الجديد والتي كتبها جيبسون عام 1986 العديد من القضايا من ناحية المصطلح في مجال لغة العالم الافتراضي لم تكن مطروحة من قبل بهذا الشكل العميق.

(2) وعلى الرغم من انتشار شبكة الإنترنت وتعدد استخداماتها ما زالت شبكة الإنترنت في مهدها، ومع عمرها القصير باتت تشكو من الاختناقات وفوضى المعلومات، وتتوالى على أسماعنا أنباء عن ظهور أجيال جديدة ومتطورة سوف تفوق ما هو قائم بقدر كبير، سواء من حيث السرعة أو الإمكانيات الفنية، حيث سيوفر =

من الوثائق الموضوعة إلكترونيًا في حاسبات مختلفة متصلة بشبكة الإنترنت[1]، والتي تتيح لأي شخص أو جهة الاطلاع على معلومات تخص جهات أخرى أو أشخاصًا آخرين قاموا بوضعها بشكل متاح للعامة، عن طريق أسلوب تكنولوجي يقوم بتنظيم البيانات والمعلومات واستدعائها[2]، وتقوم بعملية التخزين الخاصة بالمعلومات، مع القدرة على إقامة صلات وعلاقات ترابطية مباشرة فيما بينها على غرار الترابط الحاصل في نسيج الشبكة التي يصنعها العنكبوت[3].

وتستخدم الشبكة العنكبوتية لغة عالمية Hyper Text Markup Language (HTML) أي الكلمات المضيئة، وهي اللغة التي تستطيع برامج تصفح شبكة الويب قراءتها فهي من أكثر الخدمات استخدامًا في شبكة الإنترنت، ويمكن من خلالها الإبحار في مختلف المواقع على شبكة الإنترنت وتصفح ما بها من صفحات Web Page، عن طريق وسائط متعددة، قد تكون مكتوبة، أو مرسومة، أو بالصوت، أو بالصورة، وذلك من أجل الوصول إلى معلومات معينة، أو إبرام عقد مع أحد الأشخاص أو الشركات التي تعرض منتجاتها على الشبكة، وذلك عن طريق مواقع الويب Web Site، وهناك الملايين من مواقع الويب على الشبكة لكل منها

= مسارات أوسع بكثير لتدفق المعلومات، وذلك باستخدام الألياف الضوئية ذات السعة الهائلة، وبالتالي ستزداد الخدمات التي تقدم عبر شبكة الإنترنت.

(1) د. أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي، البيئي)، دار النهضة العربية، الطبعة الأولى، 2002، ص 27.

(2) د. حسام الدين الأهواني، حماية حقوق الملكية الفكرية، مؤتمر حول الملكية الفكرية، جامعة اليرموك الأردن، 10 تموز 2000، ص 19.

(3) د. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، رسالة دكتوراه، بيروت 2000، ص16.

عنوانه الخاص الذي يشار إليه بأحرف مختصرة، والذي يقوم مقام العنوان العادي أو رقم الهاتف.

وتعرف أيضًا بأنها الارتباط الدولي المتصل بشبكة حواسيب حول العالم، وكذلك تعرف بأنها نظام معلومات نشط يعمل على شبكة الإنترنت، له طابع اتصال عالمي متفاعل وديناميكي يخترق الحدود بأسلوب الربط التصويري[1].

وتعتمد الشبكة أسلوب التصفح أو الإبحار في التعامل معها، وهو نظام يستخدم للحصول على المعلومات من أي نوع (تثقيفية - تقنية - فنية - علمية - قانونية - فقهية - تجارية - اقتصادية... إلخ)، وفق ما هو متوافر على الشبكة من معلومات، ويتم التعامل عبر شبكة المعلومات الدولية باستحداث موقع أو صفحة.[2]

ويمثل الموقع مجموعة وثائق موضوعة في عنوان واحد عبر الشبكة،

---

(1) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 47 وما بعدها.

(2) لا زال يسيطر متصفح مايكروسوفت إنترنت إكسبلورر بإصداراته المختلفة 5 و6 و7 على أكبر عدد من المستخدمين رغم مزاحمة شديدة من المتصفح الرائع فايرفوكس، حيث كان عدد مستخدمي شبكة الإنترنت إكسبلورر وقت طرح متصفح الفايرفوكس في يناير من العام 2005 أكثر من 75% من إجمالي المستخدمين تاركًا 16% فقط للفايرفوكس، ومع مرور الوقت وتطوير الفايرفوكس وصل عدد مستخدميه في يوليو عام2007 م إلى 34% مزاحمًا الإنترنت إكسبلورر الذي انخفض عدد مستخدميه إلى 58%، طبعًا لم يترك هذا التنافس أي مجال سوى الفتات للمتصفحات الأخرى أوبرا، وسفاري وموزيلا، حيث لا تتجاوز حصتهم من الكعكة 2% لكل منهم! ونعتقد بأن نجاح شبكة الإنترنت إكسبلورر في الحفاظ على هذه الحصة الكبيرة من الكعكة ليس إلا بسبب وجوده ملحقًا بنظام الويندوز حاله حال برامج مايكروسوفت الأخرى الملحقة. www.internetworldstats.com

فهو إذًا بيئة إلكترونية في جغرافية افتراضية على الشبكة الدولية قد يتضمن نصوصًا، ورسومات، وصوتيات، ومرئيات، وتحتوي المواقع على عدد كبير من الصفحات.

أما الصفحات فإنها تختلف عن المواقع في أنها متخصصة في بحث موضوع معين، وهي لا تعد ولا تحصى على شبكة الإنترنت، وتعرف الصفحة بأنها: ملف بيانات يتضمن أسماءً وكلمات ورسائل وصورًا وأصواتًا ووصلات نشطة لمعلومات أخرى، والصفحة إما أن تكون صفحة رئيسية بمعنى أنها تمثل مقدمة لصفحات أخرى، أو صفحة عادية تكون بداخل الصفحة الرئيسية، ويمكن التنقل والإبحار من صفحة لأخرى بفضل اكتشاف الروابط النشطة، فيتمكن المستخدم من التنقل للحصول على المعلومات المطلوبة بمجرد النقر عليها، وتعد هذه الروابط النشطة من المكتشفات الأساسية في تفصيلات شبكة الإنترنت، وبمجرد استدعاء الصفحة فإنها تعاد إلى جهاز الكمبيوتر الذي قام بإصدار الأمر بمجرد تلقي الخادم طلب الاستدعاء على شبكة الإنترنت، ومن أمثلتها الصفحات القانونية والتي تتضمن أحدث أحكام المحاكم، وأهم أخبار القضايا المعاصرة، وأهم التشريعات الصادرة في الدول، والخدمات الحكومية القانونية، والكتب الحديثة في المكتبات.

الفرع الثاني

البريد الإلكتروني

يعد البريد الإلكتروني Electronic mail والذي يعرف اختصارًا بـ " E-mail " وقد تم اكتشافه عام 1981 على يد العالم الأمريكي راي توملينسون "Ray Tomlinson"[1] أول مكتشفات تقنية شبكة الإنترنت

(1) ما زال مخترع البريد الإلكتروني وواضع أسسه يقبع في الظل، كما بقيت مجهولة=

= للأكثرية من مستخدمي شبكة الإنترنت الطريقة التي اخترع بها وسيلته الاتصالية الحديثة، فمن سمع عن راي توملينسون؟
إنه مخترع البريد الإلكتروني الذي يعيش حياة عادية موظفًا في شركة أمريكية منذ أكثر من خمسة وثلاثين عامًا، دون أدنى محاولة لتعريف العالم بأنه أحد رجال التاريخ، ولكن توملينسون فخور بما اخترعه وهذا يكفيه، ففي شهر يوليو من العام 1982 أرسل راي توملينسون أول رسالة إلكترونية في التاريخ، وقد وصلت الرسالة إلى العنوان الذي أرسلت إليه على الفور، وقد أرسلها راي لنفسه، ولا يذكر توملينسون ما كانت تحتويه الرسالة بالضبط، كل ما يذكره أنها كانت تجميعًا لعدد من الأحرف التي كتبت في صورة عشوائية مكونة كلمة (QWERTYUIOP) أو شيء من هذا القبيل.
تخرج راي في العام 1965 من معهد ماساشوستس للتكنولوجيا، وهو واحد من أشهر المراكز العلمية في العالم، وعمل بعد ذلك ضمن فريق شركة (بي بي إن) في ولاية ماساشوستس الأمريكية، ومنذ ذلك التاريخ والأحداث تبدو وكأنها رتبت نفسها بحيث تقوده إلى إحدى المصادفات التاريخية الاستثنائية، إذ قادت هذه المصادفات توملينسون نحو اختراعه الذي لم يكن مطلقًا ضمن جدول أعماله، وذلك بعكس بقية اختراعاته التي كانت تخضع للدراسات المسبقة، وكان يقوم بها إما عن سابق إصرار، أو بطلب من الشركة التي يعمل لديها.
اختارت وزارة الدفاع الأمريكية شركة (بي بي إن) التي يعمل فيها توملينسون لتقوم ببناء (أربانت)، ARPANET، وهي الأحرف التي ترمز إلى الشبكة التي تربط المعاهد العلمية والجامعات في الولايات المتحدة الأمريكية بعضها ببعض، وتجعلها على اتصال فيما بينها فقط، وذلك على غرار الشبكات المحلية التي تربط بين أجهزة الكمبيوتر في مؤسسة واحدة حاليا، واليوم يطلق على تلك الشبكات المحلية الأولى اسم (جدة شبكة الإنترنت)، فقد كانت تلك هي الشكل الأول أو التجربة الأولى لما أصبح يعرف اليوم بشبكة الإنترنت، فشبكة اليوم هي ابنة (جدة شبكة الإنترنت) الشرعية، شارك توملينسون في تصميم تلك الشبكة ببرنامج بسيط لكتابة الرسائل يدعى SNDMSG، وذلك لكي يتمكن العاملون عبر شبكة (أربانت) من أن يتركوا من خلاله رسائل لبعضهم البعض الآخر، وهذا البرنامج لا يرقى إلى مستوى البريد الإلكتروني الحالي بطبيعة الحال، ولكنه كان خطوة مهمة في =

التي أمكن تحقيقها، وقد أحدثت هذه التقنية ثورة حقيقية في عالم الاتصالات، وسوف نتعرض في هذا الفرع لتعريف البريد الإلكتروني وعناصره وأنواعه.

أولا: تعريف البريد الإلكتروني:

يمكن تعريف البريد الإلكتروني بأنه تلك الوثائق المرسلة والمستلمة بواسطة نظام بريدي إلكتروني، كما يمكن إضافة مرفقات لتلك الرسائل يتم إلحاقها بالرسالة ذاتها (Attachment) لإرسالها لأي مكان في العالم وكذلك استقبالها، بحيث يستطيع المستخدم إرسال الرسائل الإلكترونية واستقبالها من وإلى شخص أو عدة أشخاص من مستخدمي شبكة الإنترنت[1] خلال ثوان، وتتم هذه الخدمة غالبًا بالمجان[2]، فالبريد الإلكتروني يستخدم شبكة الإنترنت كصندوق بريد.

ويعد البريد الإلكتروني وسيلة في غاية الأهمية، حيث إنه يوفر للشركات وسائل اتصال بالمنتجين، وإعلام العملاء بالمنتجات المختلفة والعروض الجديدة، حيث إن الإرسال لا يحتاج إلى أي متطلبات كثيرة

= الطريق إليه، وأهمية هذا البرنامج أنه يصنع ملفا توضع فيه الرسالة, وهو ما يعني أنه لا يستعمل إلا بين شخصين أو أكثر يشتركون في جهاز كمبيوتر واحد من تلك الأجهزة التي كانت متوافرة في المعاهد والجامعات المشتركة بشبكة أربانت, فالكمبيوترات الشخصية لم تكن قد ظهرت بعد، حيث كان عليه أن ينتظر حتى عام 1981 لتظهر معجزة التحول الأكبر في عالم التكنولوجيا الحديثة التي تسيطر على عالمنا اليوم. http://www.bintnet.com/club/showthread.php?t=33709

http://ar.wikipedia.org/wiki

(1) Lillian Edwards & Charlotte Waelde، law and internet Framework of electronic commerce، HARF publishing Oxford second Edition،2000 p3

(2) د. فاروق حسين، البريد الإلكتروني، الهيئة العامة للكتاب، 1999، ص 9.

مقارنة بالبريد العادي، فهو لا يحتاج إلى الطوابع البريدية ولا يخضع لرقابة الدول، ولا يحمل مخاطر الرسائل العادية.

ويعتبر البريد الإلكتروني وسيلة من وسائل تكوين الرأي العام وقياسه؛ لأنه يعطي صلاحية التعبير عن الآراء لكل شخص تجاه قضايا وطنه والقضايا العالمية والأحداث العالمية في المجالات المختلفة، كما يتيح استطلاع آراء المواطنين في الأحداث المهمة في أوطانهم أو في العالم.

وخدمة البريد الإلكتروني تعد الخدمة الأكثر رواجًا عبر شبكة الإنترنت، وذلك لكونه يرتبط بكافة تحركات مستخدم شبكة الإنترنت في شتى أشكالها وصورها، ويجب أن يكون لكل مستخدم عنوان خاص به.

يتكون عنوان البريد الإلكتروني من أربعة أجزاء رئيسية: وهي الاسم أو اسم المستخدم بالإضافة إلى علامة آت @، مع تحديد اسم الدومين " Domain Name "، ونهاية اسم الدومين مثل COM أو NET[1].

ثانيًا: أنواع البريد الإلكتروني:

1) الويب ميل "Web Mail " وهو البريد المعروف للجميع، ويستخدم عبر شبكة الإنترنت من خلال أي متصفح ومن أي مكان في العالم، ومثال على هذا النوع بريد HOTMAIL[2] وهي خدمة بريد

(1) Peter Schnaitman، Building a Community Through Workplace E.mail: The New Privacy Frontier،2001 ،p 5، at:
http://www.mttlr.org/volfive/schnaitman.html

(2) البريد الساخن أو المسمى بالهوتميل هو أكثر ما يستخدم من أنواع البريد حول العالم، وهو تابع لشركة ميكروسوفت الأمريكية، وهو ضمن بيئة ويندوز التشغيلية، وخلف هذا البريد الساخن قصة نجاح شخصية تستحق أن نذكرها وخصوصًا أنها كما يبدو من اسم بطلها أنه مسلم، فصاحب هذا الاختراع هو: صابر باتيا، هندي الجنسية, ففي عام 1988 قدم صابر إلى أمريكا للدراسة في جامعة ستانفورد، وقد=

إلكتروني مجاني من خلال موقع MSN.

2) بريد Forwarding وهو البريد الذي يوصل الرسالة البريدية من

= تخرج بامتياز مما أهله للعمل لدى إحدى شركات شبكة الإنترنت مبرمجًا، وهناك تعرف على شاب تخرج في نفس الجامعة يدعى: جاك سميث، وقد تناقشا كثيرًا في كيفية تأسيس شركتهما للحاق بركب شبكة الإنترنت، وكانت مناقشاتهما تلك تتم ضمن الدائرة المغلقة الخاصة بالشركة التي يعملان بها، وحين اكتشفهما رئيسهما المباشر حذرهما من استعمال خدمة الشركة في المناقشات الخاصة، عندها فكر صابر في ابتكار برنامج يوفر لكل إنسان بريده الخاص، وهكذا عمل سرا على اختراع البريد الساخن وأخرجه للجماهير عام 1996، وبسرعة انتشر البرنامج بين مستخدمي شبكة الإنترنت لأنه وفر لهم أربع ميزات لا يمكن منافستها، والمميزات هي كما يلي: أن هذا البريد مجاني فردي سري ومن الممكن استعماله من أي مكان بالعالم.

وحين تجاوز عدد المشتركين في أول عام العشرة ملايين بدأ يثير غيرة (بيل جيتس) رئيس شركة ميكروسوفت وأغنى رجل في العالم، وهكذا قررت ميكروسوفت شراء البريد الساخن وضمه إلى بيئة الويندوز التشغيلية، وفي خريف 97 عرضت على صابر مبلغ 50 مليون دولار، غير أن صابرًا كان يعرف أهمية البرنامج والخدمة التي يقدمها فطلب 500 مليون دولار، وبعد مفاوضات مرهقة استمرت حتى 98 وافق صابر على بيع البرنامج بـ 400 مليون دولار على شرط أن يتم تعيينه كخبير في شركة ميكروسوفت، واليوم، ينتسب إليه يوميا ما يقارب 3000 مليون شخص مستخدم حول العالم، أما صابر فلم يتوقف عن عمله كمبرمج، بل كان من آخر ابتكاراته برنامج يدعى (آرزو) يوفر بيئة آمنة للمتسوقين عبر شبكة الإنترنت، وقد أصبح من الثراء والشهرة بحيث استضافه رئيس أمريكا السابق بيل كلينتون والرئيس شيراك ورئيس الوزراء الهندي بيهاري فاجباي .

ومما يزيد من الإعجاب بشخصية صابر أنه ما أن استلم ثروته حتى بنى العديد من المعاهد في بلاده، وساعد كثيرًا من الطلاب المحرومين على إكمال تعليمهم، حتى إنه يقال إن ثروته انخفضت بسرعة إلى 100 مليون دولار. http://www.saudistocks.com/forums/saudi9/stocks312473

عنوان إلى عنوان آخر بحيث ترسل رسالتك إلى عنوان بريدي ثم يقوم هذا الأخير بإرسالها إلى البريد المطلوب الآخر، وسوف نورد مثالا توضيحيًا لهذا النوع: إذا كان لديك بريد Forwarding فالجميع يراسلك عليه، ثم يقوم بريد Forwarding بتوصيل تلك الرسائل إلى بريد آخر لك أي أن الشخص الذي أرسل لك رسالة بريدية لا يعرف عنوان بريدك الأصلي، وهذه الطريقة تعتبر طريقة آمنة يمكنك استخدامها إذا كنت لا تريد أن يعرف أحد بريدك الأصلي.

3) بريد POP3 وهو بريد مشابه لبريد Web ولكنه يختلف عنه فقط في أنه يجب استخدام برنامج مساعد له مثل: (Outlook-MS أو Eudora أو Pegasus) ثم تقوم بإعداد تلك البرامج لإرسال واستقبال الرسائل البريدية، وهو البريد الخاص بالشركات التي تنشئه لموظفيها من خلال مواقعها على الشبكة الدولية[1].

الفرع الثالث

الاتصال المباشر

يعتبر هذا القسم من شبكة الإنترنت وسيلة التواصل بين البشر في كافة أنحاء العالم وفي كافة المجالات السياسية والاقتصادية والاجتماعية.

وقد تطور الاتصال المباشر Direct connection على إثر تعميم البريد الإلكتروني، وهي طريقة يمكن استخدامها لتبادل الأخبار والآراء والنقاش حول موضوع معين في أي مكان في العالم بين عدد غير محصور من مستخدمي شبكة الإنترنت، كما لو كان حديثًا مباشرًا بينهم.

(1) عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 50، 51.

والاتصال المباشر يتم باستخدام تقنية برمجية تسمح بالاتصال بخادم واحد من الأطراف المتصلين جميعهم، وهو ما يجعل الاتصال المباشر عبر شبكة الإنترنت مختلفًا عن الاتصال الهاتفي.

ويتميز هذا القسم بأنه يقوم بنقل الصوت والصورة في تجسيم طبيعي، بحيث يمكن لأطراف الحوار اتخاذ قرار بالتشاور فيما بينهم، وإذا كان لهذا القسم من شبكة الإنترنت مزايا وفوائد متعددة إلا أنه يحمل في الوقت ذاته خطورة؛ إذ إنه أهم وسيلة لارتكاب الجرائم عبر شبكة الإنترنت، مثل جريمة السب والقذف والتهديد والإخلال بالآداب العامة، فتتم الجريمة في لحظة معينة نظرًا للتواجد المباشر بين الجاني والمجني عليه أو بين الجناة بعضهم البعض.

ويوفر وجود الخادم طريقة لتحصيل الدليل من خلال حفظ ملف يحتوي على نوعية الجريمة المرتكبة ومرتكبيها.

وختاما لهذا التقسيم الثلاثي, والذي نؤيد القول بعدم وجود أقسام أخرى للإنترنت سواها, وأن ما ذكر من آراء تكاد تندرج ضمن التقسيم الثلاثي, نستطيع القول بأننا وصلنا إلى القول بمدى أهمية هذا التقسيم على اعتبار أنه يمثل بيئة شبكة الإنترنت وما هي عليه حتى اللحظة، ومن غير المتصور وجود قسم آخر للإنترنت حاليا لكن من الممكن ظهور أقسام أخرى في المستقبل.

كما ترجع أهمية ذلك التقسيم إلى أنه يحقق أكثر من فائدة، فهو يساعد مستخدم شبكة الإنترنت على التركيز في الغرض الذي من أجله يستخدمها، ويجعله يلم بهذا القسم إلمامًا تامًا، كما يساعد هذا التقسيم العاملين في مجال تطوير شبكة الإنترنت على فهم البدائل التي توفرها شبكة الإنترنت وتلقى قبولا لدى مستخدميها، مع إمكان تطوير هذه الأقسام سواء بالإضافة أو

باستحداث أقسام جديدة تمامًا، كما أن تقسيم الإنترنت يسهل من التوسع في التخصص ليس فقط على مستوى إعداد البرمجيات وإنما في إطار الاستخدام، ويساعد التقسيم على تحديد الوسيلة التي يتم بها ارتكاب الركن المادي في جرائم شبكة الإنترنت، سواء أكان ذلك في صورة نشر إلكتروني أو رسالة بالبريد الإلكتروني أو بالاتصال المباشر.

ولم يسلم تقسيم الإنترنت من الانتقادات، والتي من أهمها أنه يمثل ما هو موجود حاليًا ولا يمثل منتهى الحركة فيها، فقد تتزايد هذه الأقسام بتزايد معدلات حركة الاستخدام، كما أنه لا توجد فواصل كلية بين الأقسام الثلاثة[1]، بل هي متداخلة فيما بينها حيث يستطيع مستخدم شبكة الإنترنت أن يتصفح وفي الوقت ذاته يرسل رسالة إلكترونية ويتحادث مباشرة مع أشخاص في دول أخرى.

المطلب الرابع

خصائص الإنترنت

تتميز الإنترنت - باعتبارها وسيلة التواصل بين الشبكات - بخصائص محددة، فهي تتجاوز الحدود الجغرافية إلى العالم الافتراضي، كما أنها ترتبط ارتباطًا وثيقًا بالحواسب أو أجهزة الكمبيوتر، وأخيرًا فإنها ذات طبيعة تقنية إنسانية، كل ذلك جعل لها تأثيرًا اجتماعيًا واقتصاديًا ذا طابع عالمي، وسوف نتناول بالدراسة في هذا المطلب تلك الخصائص، وذلك من خلال ثلاثة فروع:

الأول: ارتباط الإنترنت بجهاز الكمبيوتر، **والثاني:** تحرر مستخدم

(1) فادي محمد عماد الدين توكل، عقد التجارة الإلكترونية، رسالة ماجستير مقدمة لكلية الحقوق جامعة القاهرة، دار النهضة العربية، 2008، ص 8.

الإنترنت من قيود التقنية، والثالث: التأثير الاجتماعي والاقتصادي للإنترنت:

الفرع الأول

ارتباط الإنترنت بالحاسوب

تعد شبكة الإنترنت إحدى تقنيات الحوسبة المتطورة، بحيث لا يمكن تصور وجود شبكة الإنترنت بدون تقنية الكمبيوتر، وعلى الرغم من ذلك الارتباط فإنه من الضروري التأكيد على أن الكمبيوتر ليس هو شبكة الإنترنت، كما أن الإنترنت ليست هي الكمبيوتر، ويقتضي هذا الارتباط بحث موضوع الحاسوب ومكوناته وخصائصه.

1 - معنى الحاسوب:

كلمة كمبيوتر Computer مشتق من الفعل Compute بمعني يحسب، ويعرف الحاسوب بأنه آلة حاسبة إلكترونية ذات سرعة عالية ودقة متناهية، يمكنها معالجة البيانات Data Processing وتخزينها Storing واسترجاعها Retrieval وفقًا لمجموعة من التعليمات والأوامر للوصول للنتائج المطلوبة[1]، ويعد الحاسوب من الآلات الإلكترونية Electronic devices التي تقوم بمجموعة مترابطة ومتتالية من العمليات على مجموعة من البيانات المدخلة Input Data تتناولها بالمعالجة وفقًا لمجموعة من التعليمات Instructions والأوامر الصادرة إليه، والمنسقة تنسيقًا منطقيًا حسب خطة موضوعة Algorithm مسبقًا لحل مسألة معينة، بغرض

(1) L. Jean Camp & D. Riley, "Protecting an unwilling electronic populace", Proceedings of the Fifth Conference of Computers Freedom and Privacy, 28،31 March 1995, San Francisco, CA, pp. 120،139.

الحصول على نتائج ومعلومات تفيد في تحقيق أغراض معينة، وتسمى التعليمات والأوامر بالجمل Statements، ومجموعة الجمل هذه تسمى برنامجًا Program، والشخص الذي يصمم البرنامج يسمي مبرمجًا Programmer.[1]

2 - مكونات الحاسوب:

تنقسم مكونات الحاسوب إلى قسمين: القسم الأول مجموعة من الأجهزة الإلكترونية تسمى المعدات Hardware، يتم التحكم في أدائها بواسطة مجموعة من البرمجيات Software وهي التي تشكل القسم الثاني، ونرى إضافة قسم ثالث له أهميته التي لا تقل عن أهمية القسمين المذكورين خصوصًا بعد ظهور شبكة الإنترنت، وهذا القسم هو المعلوماتية أو البيانات Information data.

(1) تتعدد أنواع الحواسيب من حيث طريقة عملها وحجمها، وقد كانت أوائل الحواسيب الإلكترونية في حجم غرفة كبيرة وتستهلك طاقة مماثلة لما يستهلكه بضعة مئات من الحواسيب الشخصيّة اليوم، ومن الممكن اليوم صنع حواسيب داخل ساعة يد تأخذ طاقتها من بطارية الساعة، وينظر المجتمع إلى الحاسوب الشخصي ونظيره المتنقل (الحاسوب المحمول) على أنهما رمزان لعصر المعلومات؛ فهما ما يفكر فيه معظم الناس عند الحديث عن الحاسوب، وعلى الرغم من هذا فأكثر أشكال الحاسوب استخدامًا اليوم هي الحواسيب المضمّنة، وهي أجهزة صغيرة وبسيطة تستخدم عادة للتحكم في أجهزة أخرى، فعلى سبيل المثال يمكنك أن تجدها في آلات مختلفة مثل الطائرات المقاتلة، وآلات التصوير الرقمية ولعب الأطفال، ولا يمكن القول بأن الحاسوب هو اختراع بحد ذاته لأنه كان نتاج كثير من الابتكارات العلمية والتطبيقات الرياضية، وقد أطلق شارل باباج لفظة computer على الشخص الذي يدخل البيانات إلى الحاسوب، لكن فيما بعد أطلقت اللفظة على الآلة نفسها، وعربت هذه اللفظة بكلمة حاسوب.
http://ar.wikipedia.org/wiki

3 - خصائص الحاسوب:

يمكن إيجاز هذه الخصائص في سرعة إنجاز العمليات، وسرعة إدخال البيانات واسترجاع المعلومات، والقدرة على تخزين المعلومات، ودقة النتائج التي تتوقف أيضًا على دقة المعلومات المدخلة إليه، وتقليص دور العنصر البشري خاصة في المصانع التي تعمل آليًا، وسرعة إجراء العمليات الحسابية والمنطقية المتشابكة، وإمكانية عمل الحاسوب بشكل متواصل دون تعب، وتعدد البرمجيات والبرامج الجاهزة التي تسهل استخدام الحاسوب دون الحاجة إلى دراسة علم الحاسوب وهندسة الحاسوب، وإمكانية اتخاذ القرارات وذلك بالبحث عن كافة الحلول لمسألة معينة وتقديم أفضلها وفقًا للشروط الموضوعة والمتطلبات الخاصة بالمسألة المطروحة، وقابلية الربط والاتصال من خلال شبكات الحاسوب، حيث يمكن ربط أكثر من جهاز مع إمكانية نقل البيانات والمعلومات فيما بينها، كما أنه يعتبر أداة دافعة للنهضة في المجالات المختلفة كالتعليم، والاقتصاد، ووسائل التجارة، والنقل، والإدارة، والدفاع، ونظم المعلومات[1].

4- تبعة الارتباط بين الإنترنت والحاسوب:

أدى ارتباط شبكة الإنترنت بالحاسوب ارتباطًا وثيقًا إلى وجود ارتباط بين الجرائم المتعلقة بشبكة الإنترنت (Internet Crime) وبين جرائم الحاسوب (Computer Crime)، مع وجود فارق زمني فيما بين بداية ظهور كل منهما، حيث أرجع الفقه الجنائي جرائم الحاسوب إلى عام 1958، في حين بدأت جرائم شبكة الإنترنت مع بداية إطلاق شبكة

(1) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 58.

الإنترنت عام 1988[1].

ولا يزال الفقه والتشريع المقارن في حقيقة الأمر يجد صعوبة في التمييز بين جرائم الحاسوب وبين تلك الناجمة عن استخدام شبكة الإنترنت، حتى إن تقرير الأمم المتحدة عن منع الجريمة عام 1995 تحدث عن جرائم الكمبيوتر والجرائم الأخرى المرتبطة بالكمبيوتر (Computer crime & other crimes related to computer)[2].

ولن نخوض في الخلاف الفقهي حول التعريفات التي وضعت لجرائم الكمبيوتر أو جرائم شبكة الإنترنت، ولكن سنحاول اختيار التعريف الذي نرى من وجهة نظرنا أنه الأقرب للصواب.

(1) د. محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25: 28 أكتوبر 1993، ص 2.
شهد العام 1958م الحالة الأولى الموثقة لجريمة ارتكبت بواسطة الحاسب الآلي، راجع حول ذلك: د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، ص 9 وما بعدها.
وسجلت أول قضية في عالم شبكة الإنترنت في العام 1989 حيث تمكن طالب جامعي بمفرده من إتلاف معلومات 6200 جهاز كمبيوتر بشكل متعمد، وهو الطالب موريس Morris بالسنة الأولى لدرجة الدكتوراه بعلوم الكمبيوتر جامعة كورنل Cornell University. راجع حول ذلك: د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000، ص 12، ود. محمد مراد عبد الله، شبكة الإنترنت وجناح الأحداث، الأمن والإنترنت، القيادة العامة لشرطة دبي، 2001، ص21.

(2) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 1999، ص 156.

أ -تعريف جرائم الحاسوب:

عرف بعض الفقه والتشريع جرائم الحاسوب بأنها: " فعل غير مشروع موجه ضد النظام باستخدام الحاسوب كآلة، فهو موضوع الجريمة والوسيلة إلى ارتكابها، وهو في الوقت ذاته مستودع الدليل المرتبط بالجريمة ". وعلى ذلك فهي جرائم تتطلب دراية ضرورية بالحاسوب لكي يتم ارتكاب الجريمة بنجاح.

ووزارة العدل الأمريكية ذهبت إلى تعريف جرائم الحاسوب بأنها " كل ارتكاب لعدوان على أي قانون يتضمن في محتواه تقنية الحاسوب ويكون عرضة للتحقيق والاتهام"[1]، ووفقًا للتعريف الأمريكي لجرائم الحاسوب والذي استوحاه من الربط بين الحاسوب وتقنيته يوجد ثلاثة أنواع من الجرائم وهي:

- الجرائم التي يكون الحاسوب هدفًا لها، وفيها يهدف المجرم إلى سرقة بيانات من الحاسوب، أو إلحاق أضرار به أو بنظام تشغيله، أو بالشبكة التي يعمل خلالها.
- الجرائم التي يكون الحاسوب وسيلة لارتكابها، بمعنى أن المجرم يستخدم الحاسوب لتسهيل ارتكاب جرائمه مثل الاحتيال على البنوك باستخدام برمجية تحويل العملة لصالحه، فيودع مبالغ محولة لحسابه بدلا من وضعها في مسارها الصحيح.
- الجرائم التي يكون الحاسوب أداة لحفظ الأدلة دون أن يكون وسيطًا في الحصول عليها، ومن أمثلتها الاعتداء على حقوق الملكية الفكرية والأدبية الخاصة ببرمجيات بقصد استخدامها دون إذن صاحبها،

(1) Tom forester, Essential problems to High.Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104

وكذلك السرقة الإلكترونية التي تتم عدوانًا على حقوق المؤلف[1].

ب - تعريف جرائم الإنترنت:

كما عرف بعض الفقه والتشريع جرائم شبكة الإنترنت بأنها: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية والمعنوية[2]،أو على البيانات والمعلومات,[3] كما أنها ترتكب بواسطة الأداة التواصلية بين الشبكات

(1) د. أسامة الخولي، الحاسوب هذا الطفل الذي ولد كبيراً، مجلة عالم الفكر الكويتية، عدد أكتوبر، نوفمبر، ديسمبر 1987، ص2.

(2) د. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، دار النهضة العربية، 2009، ص 6.

(3) كانت المشكلة الأساسية التى واجهت الفقه والقضاء وحسمتها بعض التشريعات تتعلق بمعرفة: هل البيانات المحفوظة بالحاسبات تعد من قبيل المنقولات التى تخضع لأحكام السرقة أو النصب أو خيانة الأمانة؟ وقد أجابت التشريعات الحديثة على هذا السؤال بالإيجاب، من هذه التشريعات قانون لكسمبورج الذى قسم المنقول إلى نوعين: المنقول المادي، والمنقول غير المادي (المادة 240 عقوبات المعدلة بمقتضى هذا القانون) وبالتالى قرر أن السرقة تقع أيضًا على الأموال غير المادية (م 461 عقوبات) لذا فقد اعتبر من قبيل السرقة أن يظهر الجاني على المال غير المادي بمظهر المالك, كما اعتبر من قبيل الظروف المشددة للسرقة استعمال الوسائل الإلكترونية فى اختلاس الأموال (المادة 467 عقوبات) كما عاقب القانون على جريمتي النصب وخيانة الأمانة إذا كان محلهما أموالا غير مادية.
واعتبر المشرع من قبيل المفاتيح المصطنعة المفاتيح الإلكترونية المستخدمة فى ارتكاب السرقة، وجرّم اصطناع المفاتيح الإلكترونية (المادتان 487، 488 عقوبات), وتبقى المشكلة قائمة في القوانين الأخرى التي لم تستحدث نصوصًا في هذا المجال على نحو يضفي حماية جنائية شاملة.
انظر حول ذلك: د. محمد أبو العلا عقيدة, الحماية الجنائية للتجارة الإلكترونية, مؤتمر مكافحة جرائم تقنية المعلومات, جامعة الشارقة, كلية القانون 26-30 =

(الحاسوب) دون اعتبار للحدود الدولية[1].

ونظرًا للارتباط بين الإنترنت والحاسوب فإنه توجد صعوبة في الفصل بين جرائم الحاسوب وجرائم الإنترنت.

الفرع الثاني

تحرر مستخدم الإنترنت من القيود التقنية

ترتكز شبكة الإنترنت على تقنية الحاسوب، فهي عبارة عن برامج عمل متطورة تجعل التواصل مع المعلومات ممكنًا وسهلا، ذلك أن وضع الأسس الأولى للإنترنت تم من خلال البرمجة عبر الحاسوب، فهي مرتبطة ارتباطًا وثيقًا به، مع انفرادها بنظام تقني خاص (كلغة شبكة الإنترنت) رغم أن برمجتها تتم عبره، والحقيقة أنها تمثل ثورة علمية وتقنية اجتماعية واقتصادية بالمعنى الحقيقي للكلمة قلبت المعايير السائدة رأسًا على عقب، كما أنها تقنية جامحة ليس لها من مروض في مجالها سوى الاستمرار في البحث عن فوائد أخرى باستمرار يمكن أن تتحقق للبشرية، فإذا كانت تقنية الحاسوب قد منحت الإنسانية انشطارًا تقنيًا فإن على الإنسانية أن تدرك أن هذا ليس نهاية المطاف.

وحتى عام 1991 لم تكن شبكة الإنترنت شائعة الاستعمال، وإنما كانت تقتصر على الممارسين للحاسوب، كما أن مستخدميها كانوا يخضعون لنظام أمني محدد، ولكن بعد سقوط الاتحاد السوفيتي تخلصت شبكة الإنترنت من السرية، وأصبح مستخدموها يتزايدون يومًا بعد يوم، مما أدى إلى سهولة

= نوفمبر 2006, ص14.

(1) ورد هذا التعريف في المؤتمر الدولي الأول لقانون الإنترنت بالغردقة 21: 25 أغسطس 2005.

استخدامها وسهولة تطويرها.

فشبكة الإنترنت سهلة الاستخدام والاستعمال طالما كان هناك حد أدنى من القدرة على استخدام تقنية الحاسوب نظرًا لأنها تقنية ليست بعيدة المنال عن المعرفة الإنسانية العامة، بل أمكن للعامة استخدام تلك التقنية عبر الأوامر الصوتية دون الحاجة إلى تشغيل الجهاز بالمعرفة التقنية، كما أن غالبية مستخدمي شبكة الإنترنت ليس لهم دراية كبيرة باستخدامات الحاسوب وإنما بتشغيله في نطاق ضيق فقط، ومع ذلك فإنهم يملكون القدرة على الإبحار عبر شبكة الإنترنت من خلال أقسامها الثلاثة[1].

وإذا كان التعامل مع شبكة الإنترنت يحتاج إلى قدر من العلم والدراية بتقنيتها فضلا عن تقنية الحاسوب، فإنه يمكن للمستخدم أن يتعلم ذلك تعليمًا ذاتيًا دون حاجة إلى الدراسة في معاهد متخصصة.

كما أن شبكة الإنترنت سهلة التطوير، فبعد أن تحررت من قيود السرية عقب سقوط الاتحاد السوفيتي كما ذكرنا أصبح مجال تطويرها مفتوحًا أمام كل من يمتلك أفكارًا مبدعة، فلم يعد مقصورًا على طائفة العلماء، ومما ساعد على ذلك اللامركزية التي تتمتع بها شبكة الإنترنت، حيث أضحى كل من يملك أفكارًا جديدة يمكن أن ينفذها عبرها، فشبكة الإنترنت تعد بحق المجال الخصب للأفكار العلمية الجديدة سواء في مجال التعامل بها أو في مجال استخدامها[2].

على أنه يلاحظ أن هذه السهولة في التطوير تحمل معها جانبها السلبي،

(1) د. عبد الفتاح بيومي حجازي،جرائم الكمبيوتر والإنترنت في التشريعات العربية، مرجع سابق، ص 30.
(2) د. محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، مرجع سابق، ص 60.

ففي الوقت الذي يتم فيه تطوير شبكة الإنترنت في مجالات التعامل والخدمات فإنه كذلك وبالسهولة ذاتها يتم تطوير أنظمة اختراق الشبكات للولوج إلى داخلها، والتحايل على طرائق التشفير في محاولة لفك الحصار الأمني المشيد حول تلك الشبكات، وإن كانت هذه الأمور السلبية تحتاج إلى إعداد وتفكير وإدراك للتقنية المتطورة للحاسوب وشبكة الإنترنت في درجاتها العالية، والذي قد يصل إلى حد ارتكاب الجرائم.

ومع ذلك فإن هذا الاستخدام العقلي للتقنية الحديثة قد يؤدي في نهاية الأمر إلى تطوير شبكة الإنترنت، وهو ما دفع بعض الشركات الكبرى في سبيل تحقيق مصلحتها وتفادي ارتكاب الجرائم أن تسعى إلى التعاقد مع هؤلاء للاستفادة منهم كتقنيين تجنبًا لارتكابهم أفعالا غير مشروعة عبر شبكة الإنترنت.

الفرع الثالث

التأثير الاجتماعي والاقتصادي للإنترنت

رأينا أن شبكة الإنترنت كانت ردة فعل غربية تجاه التطور العلمي والعسكري للكتلة الشرقية، وكانت من القوة بحيث أدت إلى انكسار ذلك التطور العسكري.

وقد أحدثت هذه التقنية الجديدة تحولات في الأفكار السائدة، حتى إنها امتدت لتصل إلى صناع القرار السياسي في كل دولة، بل امتد هذا التأثير ليصبح عالميًا من الناحية الاجتماعية والاقتصادية.

فمن الناحية الاجتماعية برز تأثير شبكة الإنترنت كظاهرة عالمية على المجتمع الدولي والإقليمي بل والمحلي أيضًا، فالحياة تبدو أكثر سهولة عبر شبكة الإنترنت؛ حيث إنها تعد مجالا استقطابيًا نشطًا، ووسيلة علمية ممتعة

لفتح مجالات جديدة، إذ أصبح في مقدور الباحث الحصول على المعلومات المطلوبة بمجرد إجراء عملية بحث search حيث يتم رصد كافة البحوث والموضوعات المتعلقة ببحثه طالما وجدت لها مكانًا على شبكة الإنترنت، فظهرت إلى الوجود لغة جديدة تستخدم حروف ومطلحات جديدة لا يفهمها سوى مستخدم الانترنت فقط, الأمر الذي من شأنه أن ينعكس سلبا على المجتمع ولغته, بالإضافة لوجود عدة آثار اجتماعية أخرى انعكست على المجتمع من جراء استخدام الانترنت واعتماد الحياة على التقنية بدرجة كبيرة.

ومن الناحية الاقتصادية برزت شبكة الإنترنت بقوة في المجال الاقتصادي، ويمكن القول إجمالا أنه منذ بداياتها أصبحت مؤثرة في الاقتصاد العالمي، فحتى سنة 2000 كان حجم التجارة عبر شبكة الإنترنت ثلاثة تريليون دولار أمريكي، وأصبح مصطلح التجارة الإلكترونية Electronic Commerce يتم تداوله بشكل مكثف، فالتجارة الإلكترونية حقيقة واقعة الآن[1] على الرغم من وجود بعض المشكلات التقنية التي تواجهها.

والجدير بالذكر في هذا المقام الإشارة إلى أن مفهوم التجارة الإلكترونية لا يقتصر على عرض السلع كما هو الشأن في حالة استخدام الأجهزة التقليدية كالراديو Radio والتلفزيون TV[2]، بل امتد إلى إمكانية تداول السلع والخدمات عبر شبكة الإنترنت، وفي الوقت ذاته أصبح من اليسير الحصول على نظام خدمي متكامل؛ إذ يمكن متابعة البورصة العالمية

(1) http://www.grolier.fr/cyberlexnet/com/a98099902.htm

(2) وهو أسلوب عرض السلع والتسوق عبر شاشات التلفزيون, وأيضًا الإذاعة المسموعة الذي بدأ أول مرة في فرنسا.

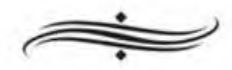
لمعرفة تطورات الأسعار وتبادل الأسهم، فالمتابعة وقتية وليس هناك فارق في الزمن.

وأكثر ما يدل على التأثير الاقتصادي لشبكة الإنترنت أنها سمحت بظهور أفكار اقتصادية جديدة ومنها ظهور المحل الإلكتروني E-store وهو ما يجد رواجًا في التعامل عبره كنشر المؤلفات وبيعها.

ولعل من أهم ما صاحب شبكة الإنترنت وتأثيرها في الاقتصاد هو دراسات حماية المستهلك Protection des consommateurs والتي بدأت تأخذ أبعادًا وقائية أكثر من مجرد الإلزام القانوني، وذلك بالإرشاد والتوجيه وتقنين السلوك عبر شبكة الإنترنت.

إن المبادئ الجديدة التي تضعها شبكة الإنترنت في الفكر الاقتصادي لا تحكمها أفكار مسبقة، بل تنهض على مبدأ المساواة بين جميع أعضاء شبكة الإنترنت، فليس من مفاضلة بينهم إلا لمن يملك القدرات الفنية والتقنية ومن يتفاعل مع التطور العلمي الذي لا يمكن التراجع عنه.

وعلى الرغم من التحولات الاجتماعية والاقتصادية الإيجابية التي استهدفتها شبكة الإنترنت فإن هذه التحولات صادفت وجود نقيضها السلبي، مما أدى إلى تصدي الفقه والقضاء في النظم المقارنة للبحث في إمكانية إيجاد مواءمة بين النظام القانوني وشبكة الإنترنت.



المبحث الثاني

قانون الإنترنت (Cyber Law)

أثارت مسألة تحديد نطاق قانون الإنترنت جدلا فقهيًا، خصوصًا بوجود مصطلح جديد هو العالم الافتراضي cyber space، وعلى الرغم أنه لم يخضع حتى الآن لدراسات كافية يمكن أن تكون نواة تصنع الغائب وتضعه في أول الطريق، إلا أن الفقه المقارن شرع في بحث مسألة تحديد العالم الافتراضي كحقيقة باعتباره العالم الذي خلقته شبكة الإنترنت ليكون أرضًا جديدة يخترقها الإنسان دون أن يكون له عليها من سلطان، ورغم ذلك فما هو موجود من حركة فقهية وتشريعية ربما تكون قد التقت جميعها في محاولاتها لمد سلطان القانون إلى الأرض الجديدة التي تستلزم التأهيل النفسي للأفراد والشعوب.

وقد برز اتجاهان في إطار تفعيل فكرة القانون في ذلك العالم الافتراضي: الأول هو الاتجاه المجازي، والثاني هو الاتجاه الوظيفي[1]، وسوف نتناول دراسة هذا المبحث من خلال أربعة مطالب:

المطلب الأول: تعريف قانون الإنترنت

المطلب الثاني: مدارس قانون الإنترنت

المطلب الثالث: خصائص قانون الإنترنت ومراتبه

المطلب الرابع: أقسام قانون الإنترنت.

---

(1) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 104.

المطلب الأول

تعريف قانون الإنترنت

نتناول في هذا المطلب التعريف الفقهي لقانون الإنترنت ونطاقه واتجاهات التفسير:

ونعني بعبارة قانون الإنترنت Cyber law ذلك الفرع من فروع القانون الذي يتناول بالتنظيم الإنترنت كوسيلة أو أداة تواصلية بين الشبكات دون اعتبار للحدود الدولية، فهو يشير إلى النطاق القانوني للإنترنت باعتباره مصطلحًا مبتكرًا يشير إلى ذلك الفرع من فروع القانون الذي يهتم بالموضوعات القانونية المرتبطة بشبكة الإنترنت وخدمات الاتصالات.

عندما برزت على المستوى الفقهي مسألة نطاق الإنترنت وحدودها Cyber spatial في مصطلح جديد كل الجدة هو العالم الافتراضي Cyber space والذي يعود الفضل في ربطه بشبكة الإنترنت إلى البروفيسور John Perry Barlow[1] مستندًا إلى الدعم المجازي لأفكار

(1) جون بيري بارلو John Perry Barlow كاتب كبير، وضع إعلان استقلال العالم الافتراضي في 8 فبراير 1996 في دافوس في صيغة رسالة موجهة إلى الحكومات (وليس الدول)، من مواليد مقاطعة سابلت Sublette County بولاية Wyoming عام 1947, خريج جامعة .Wesleyan Uni في Middletown بولاية Connecticut في الديانات المقارنة عام 1969, ومؤسس منظمة الحدود الإلكترونية Electronic Frontier Foundation , وعضو مركز بيركمان للإنترنت والمجتمع Berkman Center for Internet & Society بكلية الحقوق بجامعة هارفارد Harvard Law School، وهو واضع إعلان استقلال العالم الافتراضي الذي يشكل أساس مدرسة التنظيم الذاتي للإنترنت Self،regulation.

A Declaration of the Independence of Cyberspace by John Perry Barlow

Governments of the Industrial World, you weary giants of flesh and

steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is

no matter here.
Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.
In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.
You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.
In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.
Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.
These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over

الأدب المعلوماتي في رواية الأديب الكندي/ الأمريكي William Gibson - (The New romancer)، عند ذلك شرع الفقه في بحث مسألة تحديد هذا المصطلح، وقد وصل الفقه المقارن إلى مسألة العالم الافتراضي كحقيقة باعتباره العالم الذي خلقته شبكة الإنترنت ليكون أرضًا جديدة يخترقها الإنسان دون أن يكون له عليها من سلطان، وفي محاولة لامتداد سلطان القانون إلى الأرض الجديدة، برز اتجاهان في إطار تفعيل فكرة القانون في ذلك العالم الافتراضي: الأول هو الاتجاه المجازي، والثاني هو الاتجاه الوظيفي.

أولا: الاتجاه المجازي **Metaphorical**:

يأخذ الاتجاه المجازي في تحديد نطاق شبكة الإنترنت بأنه مكان خارج الحدود الإقليمية ليس له نطاق جغرافي محدد، ولكنه متوافر لكل شخص في كل مكان حول العالم، وهو اتجاه المحكمة العليا للولايات المتحدة الأمريكية في أول حكم لها يتعلق بموضوع مواءمة الدستور الأمريكي مع الحيز الذي تشغله شبكة الإنترنت أو البيئة الافتراضية Cyber spatial التي يتواجد فيها العالم الافتراضي وهي قضية Reno v. ACLU[1]، باعتبار أنها

---

our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland February 8, 1996

http://homes.eff.org/~barlow/Declaration.Final.html

(1) Reno v. ACLU: Facts of the Case

Several litigants challenged the constitutionality of two provisions in the 1996 Communications Decency Act. Intended to protect minors from unsuitable internet material, the Act criminalized the intentional transmission of "obscene or indecent" messages as well as the transmission of information

تأمـل في أن تقبـل محـاكم الولايـات المتحـدة الأمريكيـة السـير عـلى نهجهـا في الأخـذ بالاتجـاه المجازي[1]، وذلك في تحديد نطاق شبكة الإنترنت كمكان خارج الحدود الإقليمية ليس لـه نطـاق جغرافي محدد، ولكنه متوافر لكل شخص في كل مكان حول العالم.

والاتجاه المجازي يعتمد في أساسه على القياس على العالم المادي،

---

which depicts or describes "sexual or excretory activities or organs" in a manner deemed "offensive" by community standards. After being enjoined by a District Court from enforcing the above provisions, except for the one concerning obscenity and its inherent protection against child pornography, Attorney General Janet Reno appealed directly to the Supreme Court as provided for by the Act's special review provisions.

Question

Did certain provisions of the 1996 Communications Decency Act violate the First and Fifth Amendments by being overly broad and vague in their definitions of the types of internet communications which they criminalized?

Conclusion

Yes. The Court held that the Act violated the First Amendment because its regulations amounted to a content.based blanket restriction of free speech. The Act failed to clearly define "indecent" communications, limit its restrictions to particular times or individuals (by showing that it would not impact on adults), provide supportive statements from an authority on the unique nature of internet communications, or conclusively demonstrate that the transmission of "offensive" material is devoid of any social value. The Court added that since the First Amendment distinguishes between "indecent" and "obscene" sexual expressions, protecting only the former, the Act could be saved from facial overbreadth challenges if it dropped the words "or indecent" from its text. The Court refused to address any Fifth Amendment issues.

Decision: Thursday, June 26, 1997

From: http://www.oyez.org/cases/1990.1999/1996/1996_96_511/

(1) http://www.gseis.ucla.edu/iclp/internet.html

ورغم مرحلية استخدام هذا الاتجاه إلا أنه منتقد من حيث إن التفاوت كبير بين العالم المادي والعالم الافتراضي الذي خلقته ثورة التواصل الشبكي بين الحواسيب.

ثانيا - الاتجاه الوظيفي **Functional**:

يرى أنصار هذا الاتجاه أن قانون الإنترنت يتأكد وجوده في الإجابة على التساؤل: هل يُعد نطاقًا لقانون الإنترنت كل مكان يتم التواصل عبر أقسام شبكة الإنترنت الثلاثة حول العالم من خلاله؟ ووفقا لهذا الاتجاه فإن تفسير قانون الإنترنت أو التفسير الذي يتم في إطار موضوعات تتعلق باستخدام شبكة الإنترنت والتعامل بها يجب أن يأخذ طابعًا وظيفيًا مستمدًا من فهم آلية شبكة الإنترنت دون قياس من أي نوع على مظاهر العالم المادي.

الكثير من المصطلحات تفرعت عن نطاق شبكة الإنترنت أو عالمها الافتراضي، على أن أهم مصطلح تفرع عن نطاق شبكة الإنترنت هو قانون الإنترنت (cyber law)، الذي تفرع عنه الكثير من المصطلحات منها المحكمة الافتراضية (cyber tribunal) والقاضي الافتراضي (virtual magistrate)[1] والعقود الافتراضية (cyber contracts) والجريمة الافتراضية (cyber crime)، ومن أمثلتها النصب (cyber fraud) والسب والقذف (cyber defamation) والإرهاب (cyber terrorism).

وإذا ما سلمنا بظهور قانون الإنترنت (CYBER LAW) باعتباره فرعًا جديدًا من فروع القانون، وهو ذلك الفرع من القانون الذي يهتم

(1) د. سامي عبد الباقي أبو صالح، التحكيم التجاري الإلكتروني دراسة مقارنة، دار النهضة العربية، 2004، ص 185.

بالجوانب القانونية الموضوعية والإجرائية المرتبطة بشبكة الإنترنت، فقد يثار تساؤل حول مؤشرات هذا الفرع؟

لقد كان لظهور تقنية الحاسوب الأثر الأكبر على المستوى القانوني، فبدأت النظم القانونية تتفهم أهمية الحاسوب في حياة المجتمع مما أدى إلى ظهور قواعد جديدة تستوعب هذه التقنية.

وعلى الرغم من ذلك يظل السؤال الذي يطرح نفسه في هذا الموقف هو: ما مدى إمكانية مجاراة النظم القانونية المعاصرة للتطور السريع والمفاجئ الذي يطرأ على شبكة الإنترنت؟ وهي المشكلة التي تضع المشرع بين خيارات صعبة ما بين تعديل القانون بما يستتبعه من تأثير على المجتمع، وبين عدم التعديل ومن ثم عدم مواكبة تطور شبكة الإنترنت[1].

إن أهم دعائم قانون الإنترنت كفرع قانوني جديد من فروع القانون أنه يجمع في علاقة واحدة مباشرة بين أقسام شبكة الإنترنت الثلاثة، وهذا الاجتماع لن يكون له حدود يقف عندها.

ويستند قانون الإنترنت على مضمون الحرية ومفهومها حسبما هو وارد في المواثيق الدولية لحقوق الإنسان، حيث إنه ليس له نطاق جغرافي محدد، ولكنه متوافر لكل شخص في كل مكان حول العالم.

ويترتب على وجود هذه الدعامة لقانون الإنترنت أن تفسير الحقوق والالتزامات والمسئوليات سوف يأخذ مدلولا جديدًا يمزج بين الحرية الفردية والحريات العامة.

إن مصدر الصراع الرئيسي بين فقه هذا الفرع من فروع القانون وبين الفكر الاجتماعي الاقتصادي، أننا أمام بعض حريات فردية ذات صبغة

(1) الوثيقة العربية لقانون الإنترنت الصادرة عن المؤتمر الدولي الأول لقانون الإنترنت الغردقة 21: 25 أغسطس 2005.

عالمية متصفة بالتجديد تجاوزت مفهوم الدولية والإقليمية المعاصرة، يقابلها تحديات تطوير النظم القانونية لكي تتواءم معها[1]".

إن هذا التحدي القانوني يحتاج إلى أدوات يلزم توافرها لمواجهة مجتمع معلوماتي، وهو تحد لم يعد يستند إلى مفاهيم تطبيق القانون من حيث الزمان والمكان السائدة حاليًا، بل سوف يحتاج هذا المبدأ في القانون إلى إعادة تفسير، إذ إنه يتساوى أمام العالم الافتراضي الذي خلقته شبكة الإنترنت ذلك المستخدم الذي يقطن المدن أو القرى أو الضواحي أو حتى في أقصى الصحراء، فلم يعد هناك - في إطار التجريم عبر شبكة الإنترنت - ذلك القدر من التمييز بين جرائم ترتكب في مكان مأهول بالسكان كالمدن وآخر غير مأهول كالصحراء أو الريف.

بل وأبعد من ذلك فإن مسألة التمييز بين الجرائم التي ترتكب في الداخل (الجرائم ضد الأمن الداخلي للدولة) وتلك المرتكبة ضد شخصية الدولة (الجرائم ضد الأمن الخارجي للدولة) قد تكون محل جدل فقهي قانوني في هذا الإطار، بحيث يحتاج الأمر إلى قدر من المراجعة بشأنها كما هو الشأن أيضًا في المواد (من 16 إلى 25 من قانون العقوبات الاتحادي الإماراتي 3 / 1987)، والمواد (2 و3 من قانون العقوبات المصري) وفروع المادة (113 من قانون العقوبات الفرنسي).

ويطال الأمر هنا موضوع الأهلية الجنائية إذ إن من جرائم شبكة الإنترنت ذات الخطورة الخاصة ما يرتكبه قُصّر وربما أطفال لا تتوافر فيهم الأهلية، فنجدهم يخترقون أعتى النظم الأمنية ليرتكبوا جرائم ليس بدافع

(1) د. إبراهيم أحمد إبراهيم، التجارة الإلكترونية والملكية الفكرية، مجلة المحاماة، العدد الأول، 2001، ص591.

التجسس والتخابر، وإنما بدافع الفضول والزهو والشعور بالعظمة[1].

إن مسألة الحدود التي يقف عندها القانون في أي فرع من فروعه تعني بالمفهوم النظري الضيق ليس المكان الذي يقف عنده تطبيق القانون، وإنما أيضًا المكان أو النقطة التي يبدأ فيها تطبيق فرع آخر من فروع القانون، فإذا افترضنا مثلا وجود فعل غير مشروع فإن اتصافه بعدم المشروعية يعني دخوله في حيز القانون المدني كفرع من فروع القانون، أما إذا اتصف العمل غير المشروع بالجريمة لكون قانون العقوبات قد تضمن نصوصًا تجرم هذا العمل غير المشروع فإن ذلك يعني دخول عدم المشروعية في إطار حركة التجريم والعقاب بالمفهوم الجنائي، وهو الأمر الذي يجعل القانون الجنائي يتدخل لكون هذا العمل قد تخطى الحدود الجنائية هنا، لذلك فإن مسألة انتهاء حدود القانون هي مسألة ترتبط تحديدًا بفكرة تفريع القانون إلى فروع عدة سماها الفقه القانوني وعدَّد أشكالها[2].

والسؤال المطروح هنا يتعلق بالفرع الجديد الذي يحكمه قانون المعلوماتية، وهو فرع قانون تكنولوجيا المعلومات، أو كما يطلق عليه قانون الإنترنت (CYBER LAW)، كفرع جديد بدأ بالفعل يأخذ حظه من الاهتمام من قبل رجال القانون في كافة مستوياتهم التشريعية والقضائية والفقهية، فهل هناك حدود ينتهي عندها أي فرع من فروع القانون على أن تكون البداية الجديدة لقانون تكنولوجيا المعلومات، وبمعنى آخر هل هناك من دلالة تشير إلى إمكانية حدوث علاقة - ولو وهمية - بين فروع القانون

(1) د. حسن عبد الباسط جميعي، إثبات التصرفات التي يتم إبرامها عن طريق الإنترنت, دار النهضة العربية, طبعة 2000, ص 83.

(2) حسين الغافري ومحمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، 2008، ص 15.

الأخرى - ولا سيما الفرع الجنائي - وبين قانون الإنترنت، وبالعكس؟

بداية فإن المفارقة حادثة بين فروع القانون مجتمعة وبين قانون الإنترنت/ تكنولوجيا المعلومات، هذه المفارقة تتضمن أن فروع القانون المختلفة هي فروع ترتبط بوحدة النظام القانوني أساسًا، فجامعها التشريع الأعلى الذي يحكمها كالدستور والتشريعات الأساسية لكونها جميعها تستمد معالمها من عالم مادي يجد فيه البشر المعطيات والنتائج، وهو الأمر غير المتوافر في قانون الإنترنت الذي يستمد مظهره العام من عالم آخر (وهو عالم افتراضي)، ومثل هذا الأمر يجعل التمييز واضحًا بين كافة فروع القانون وبين قانون الإنترنت، بحيث يكون مبدأ قبول هذا الفرع الجديد مرتبطًا بوجود شبكة الإنترنت في المجتمع الإنساني المعاصر.[1]

بظهور شبكة الإنترنت كظاهرة إنسانية فإن هذا الفرع قد فرض نفسه على نظرية القانون ليجد له موقعًا من البداية وبشكل يستدعي قلق رجال القانون؛ حيث إنه قد فرض ذاته دون التعرف على حدوده وأبعاده وعلاقته بالفروع الأخرى على النحو المستقر المتبع في دراسات تلك الفروع.

ولا يختلف الفقه في أن مثل هذا الأمر يرتب آثارًا قانونية ذات مغزى خاص تتعلق بالتجديد، لا سيما على النحو الذي يتعلق بمكان وقوع الجريمة وزمانه، وعملية التجديد هذه تعد من الأمور الجوهرية لما يترتب عليها من تفاعل مع الامتداد الزماني للقانون كمبدأ معتمد لا سيما في نواحي مدى إمكانية تدخله، مثلما هو الحال في التقادم وغيره من المسائل التي تستلزم معرفة زمن ارتكاب الجريمة لكي يمكن ترتيب الآثار التي يقررها القانون في هذا الشأن، فمسألة العامل الزمني هذه تجعل موضوعًا كالتقادم على

(1) رأفت رضوان, عالم التجارة الإلكترونية, المنظمة العربية للتنمية الإدارية، القاهرة، سلسلة بحوث ودراسات, العدد 348, 1999, ص126.

سبيل المثال ذا خطورة في جرائم شبكة الإنترنت إذا أدركنا أن المسافة الزمنية بين دولة مثل مصر ودولة في أمريكا اللاتينية يمكن أن تصل إلى فارق يوم كامل في هذا الشأن[1].

والحقيقة أن تحديد نطاق قانون الإنترنت لم يتعرض حتى الآن لدراسة كافية يمكن أن تكون نواة تضعه في أول الطريق، فما هو موجود من حركة فقهية وتشريعية ربما تكون التقت جميعها في نطاق ضيق يرتبط بأمرين: الأول هو السعي لإثبات أحقية القضاء الوطني في نظر قضايا يكون أطراف النزاع فيها من الوطنيين، وتلك مشكلة في اعتقادنا لن تثير من قريب أو بعيد مشكلات تذكر إذا كانت الجريمة في أفضل الفروض قد ارتكبت على التراب الوطني أو في دولة لا يعاقب تشريعها على الفعل المرتكب، ففي هذه الفرضية سوف تكون كافة الآثار المترتبة على الواقعة من اختصاص القضاء الوطني إذا كان هناك تغاض واضح المعالم من قبل الفكر المصلحي هنا.

والأمر الثاني هو انتشار ظاهرة الفكر القانوني الدستوري وحقوق الإنسان وحرياته الأساسية بشكل عملي، فبدا الأمر كما لو كان هناك خطوة رائدة يقودها علماء تكنولوجيا المعلومات[2]، ومثل هذا الأمر يجعل مسيرة شبكة الإنترنت تدخل في نطاق دولي يتم فيه فرز الدول إلى قسمين كبيرين لا ثالث لهما وهما: دول تحترم حقوق الإنسان، ودول لا تحترمها.

---

(1) أيمن عبد الحفيظ، الاتجاهات الفنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، 2005، ص 20.
(2) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 110.

المطلب الثاني

مدارس قانون الإنترنت

يجمع علماء التقنية على وجود تنظيم تقني للإنترنت، إلا أن الأمر على المستوى القانوني ليس على هذا القدر من الإجماع، حيث ثار الخلاف حول إمكانية التعامل القانوني مع شبكة الإنترنت بين التأييد والمعارضة، وكذلك فيما إذا كان يكفي التنظيم القانوني التقليدي أم يحتاج الأمر إلى رؤية جديدة.

هناك أربع مدارس تاريخية ترصد تفاعل حركة القانون مع شبكة الإنترنت والعالم الافتراضي وهي: مدرسة قانون الكمبيوتر، ومدرسة قانون تقنية الإنترنت، ومدرسة التنظيم الذاتي للإنترنت، ومدرسة التنظيم القانوني للعالم الافتراضي التي لها الغلبة على ما سبقها من المدارس.

والتطور المدرسي في التفاعل مع قانون الإنترنت مرجعه - بما في ذلك تحديد أقسام هذا الفرع الجديد - هو المعيار التاريخي حتى الآن، ويكمن اكتساح المدرسة الرابعة في كونها تتعامل أساسا بالاتجاه الوظيفي وإن كانت تعترف بالاتجاه المجازي مظنة تطوير رجاله لأنفسهم، وصولا إلى التفاعل الصحيح مع وقائع شبكة الإنترنت، وبالتالي التوظيف الصحيح للقانون عليها.

والمبادئ الأساسية التي تبنى عليها مدرسة التنظيم القانوني للعالم الافتراضي ثلاثة:

أولا: البيئة التنافسية الكاملة للإنترنت: ومصدر هذا المبدأ تقرير بول باران مكتشف شبكة الإنترنت حيث إن شبكة الإنترنت يحكمها مبدآن (لا ملكية - لا مركزية).

ثانيا: أنها ظاهرة تقنية إنسانية: ومصدر ذلك أن شبكة الإنترنت تتفاعل

مع الواقع الإنساني.

ثالثا: أنها تؤمن ذاتيًا بالقطاع الفردي: ومصدر ذلك أن الفرد دون غيره هو الذي يتحكم في مصير شبكة الإنترنت، ومن الفرد يجب أن تنطلق المفاهيم، وإلى الفرد تصل المفاهيم.[1]

والملاحظ أن مدارس شبكة الإنترنت تدور جميعها حول موضوع محدد لا يكاد يخرج عن الإجابة عن السؤال التالي وهو: ما هي كيفية التعامل القانوني مع ظاهرة شبكة الإنترنت؟

والإجابة عن هذا التساؤل لا تخلو من أحد اتجاهين: الأول الاتجاه التقليدي للتعامل مع شبكة الإنترنت، والثاني الاتجاه الحديث في التعامل معه، وسوف نبين هذين الاتجاهين في هذا المطلب مع بيان الاتجاه الراجح.

أولا: الاتجاه التقليدي في التعامل مع شبكة الإنترنت:

برز هذا الاتجاه الذي يطالب بالتعامل القانوني التقليدي مع شبكة الإنترنت في العقود على وجه التحديد، فقد برزت العقود عبر شبكة الإنترنت حين التعامل مع العديد من المواقع، فإذا أراد شخص ما أن يفتتح بريدًا إلكترونيًا مجانيًا Free E-mail فإن عليه أن يوافق على العقد أو الاتفاق Agreement المطروح من قبل الشركة أو المؤسسة التي تطرح هذا النوع من الخدمة، فالعقد أو الاتفاق معد على نموذج جاهز غير قابل للنقاش أو تبادل الإرادة الموضوعية من الطرف القابل، بحيث يمكن للشركة أن تضع ما يحلو لها من شروط.

ثم تطور الأمر من العقود إلى التعليمات Instructions، فالدخول إلى بعض المواقع يستلزم الإقرار بتوافر شروط مسبقة في الشخص، كشرط السن أو الأهلية مثلا، وعلى الشخص الإقرار بمدى توافرها فيه، فإذا لم

(1) http://ar.wikipedia.org/wiki

تتوافر فيه هذه الشروط فعليه أن يمتنع عن الدخول، وهو أمر يقوم على افتراض الأمانة والمصداقية في الأشخاص مستخدمي شبكة الإنترنت، ومخالفة كل من العقد والتعليمات تجعل الشخص مسئولا وفقًا للنظم التقليدية القائمة[1].

وقد وقف هذا النوع من التعامل التقليدي عاجزًا عن التصدي لظواهر اختراق تلك النظم، لأنه يفترض أن قوة الإلزام في القاعدة القانونية تمتد إلى شخص يقيم في الإقليم ذاته الذي ينطبق فيه القانون المذكور، والحقيقة غير ذلك إذ إن من يقيم في الإمارات أو في مصر لا ينطبق عليه القانون الأمريكي أو الإنجليزي، حتى بافتراض موافقة الشخص المسبقة على انطباق قانون دولة أخرى عند موافقته على التعليمات أو الوثيقة المصاحبة، كما أن غياب الإرادة في مثل هذه النوعية من العقود الجديدة هو محل طعن وفقًا للتعامل التقليدي يستفيد منه القابل أكثر من المجاب.

ونتيجة لذلك بات التهديد بالاستخدام التقليدي للقانون لمواجهة ظواهر اختراق شبكة الإنترنت أمرًا غير ذي جدوى، لذلك لجأت بعض المواقع إلى وسائل تقنية حديثة ومتطورة مثل كلمة المرور Password وإقامة حواجز نارية Le pare-feu / Firewall.

والحقيقة التي لا مناص من الإقرار بها أنه إذا كان القانون - وفقًا لهذا الاتجاه - يستطيع القيام بتنظيم شبكة الإنترنت وتطويرها ورعايتها وحمايتها فإن السؤال الذي يمس الإشكالية هنا يتمثل في عملية الصراع الدائر الآن حول مدى قيام القانون في شكله التقليدي بهذا الدور وكيفية ذلك.

إن الإجابة الطبيعية على هذا التساؤل هي النفي، ذلك أن القاعدة

(1) الوثيقة العربية لقانون الإنترنت الصادرة عن المؤتمر الدولي الأول لقانون الإنترنت الغردقة 21: 25 أغسطس 2005.

التقليدية وقفت عاجزة حقا عن المواجهة، لذلك أطلق عليها أنها تقليدية عند بعض الفقه المؤيد للتجديد[1].

لقد تطور الأمر كثيراً - فيما يبدو - في فترة زمنية قصيرة، وإذا كان القضاء المقارن يمهد في محاولاته الجادة الطريق أمام التقنية الجديدة لمواصلة مسيرتها فإن المشرع المقارن لا يزال بطيئًا في المواجهة قياسًا على التطور التقني المتواصل والمستمر لها، وإزاء هذا انبرى الفقه القانوني المقارن في كافة المجالات للمواجهة، بل إن البعض في هذا الاتجاه نادى بضرورة الدخول في معترك التجديد الشامل للقاعدة القانونية التقليدية وليس تطويرها فحسب، وهو ما سنتعرض له في الفقرة القادمة.

ثانيًا: الاتجاه الجديد في التعامل مع شبكة الإنترنت:

برز هذا الاتجاه في فقه القانون حال صراع رجاله حول نطاق التدخل القانوني في مجال الاتصالات، كنتيجة لإقرارهم بأن التطور التقني كما أنه يستدعي التجديد في سلوكيات المعاملات في كل ظاهرة علمية جديدة، فإنه ينبغي أيضًا أن يكون التعامل القانوني على أساس هذا الجديد ومن الطبيعة ذاتها، فالاتصالات اليوم لم تعد بين شخص وآخر فحسب وإنما تطورت إلى أمر جديد، ما بين الآلة والفرد، وبين الآلة والآلة، وبين تجمعات من هذه وتلك تتحادث كلها وتتراسل فيما بينها، والتجديد هنا موقعه التغيير في أسس المعرفة ذاتها، وهذا أمر على درجة كبيرة من الخطورة إذا لم يصاحبه تطور في تنظيم عملية التغيير ذاتها.

والقانون بطبيعته - كأحد العلوم الاجتماعية التي تتفاعل مع البيئة - يتمتع بخاصية القابلية للتغيير والتجديد محافظة على ذاته، إذ بدون هذه

(1) سامر محمد سعيد، الإنترنت المنافع والمحاذير، دار سعاد الصباح، الكويت 1988، ص 27.

الخاصية فإنه يفقد معناه، ولقد ذهب البعض في هذا الشأن إلى رأي يعد موضع تأمل من حيث إمكانية إدماج فصل جديد في القانون الجنائي القائم يتعامل مع تقنيات الحاسوب، وهو أمر قبله المشرع المقارن متجاوزًا الصراع الفقهي حول هذه النقطة تحديدًا، ومن ذلك المشرع الفرنسي في قانون العقوبات النافذ عام 1994[1].

وتعد عملية التشريع المنظمة لظاهرة جديدة لأول مرة من الأمور الصعبة إلا أنها ليست مستحيلة، فقد واجه آباء القانون أمورًا أشد ضراوة من قبل، بل إن سبب الصعوبة في المواجهة تجاه عملية التشريع الجديد أن الظواهر الجديدة لم تعرف سلوكياتها بعد، وفيما إذا كانت تحتاج إلى سلوكيات جديدة أم أنه يكتفى بالسلوكيات القائمة للتعامل معها، أم أن كل ما يلزم هو تطوير القائمة، فالمسألة فيما يبدو من حيث ضرورة التوصل إلى اقتناع السلوك البشري أولا بالمنهج الجديد حتى يمكن إحداث تدخل قانوني بشأنه.

ولعل المثال الحيوي هنا هو انتقال البشرية من العصر الزراعي إلى العصر الصناعي، فقد أمكن للمجتمع الإنساني أن يصنع خطوة رائدة تجاه تقنين موحد لبعض مظاهر التطور الصناعي، ففي فترة وجيزة بعد اختراع الطائرة قام المجتمع الإنساني بوضع اتفاقيات تتعلق ببعض الجوانب ذات التأثير الكبير فيها، وكان الهدف من هذا هو توعية العالم بهذه الظاهرة العلمية، فقد كان المجتمع الإنساني يضع تشريعًا يتعامل مع ظاهرة تقنية

(1) Law number 90،1170 published in the December 30,1990 journal official
مشار إليه لدى: د. عمر محمد أبو بكر بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مرجع سابق، ص 96.

جديدة تمامًا عليه لم يكن يعرف سلوكيات التعامل معها، ثم امتد ذلك الأثر إلى نظم القانون الوطنية في معالجة هذه الظاهرة التقنية، وقد استلزم ذلك الكثير من الوقت نظرًا لأن الاقتناع الإنساني مسألة تحتاج إلى وقت.

ويبدو أن فلسفة التغيير تسود بقوة في الفكر البشري طالما هو يعبر عن حاجته بالكم والكيف معًا، وهذا أمر لا يختلف عليه اثنان، والحقيقة أن الاتجاه الذي سوف يكتب له السيادة هو ذلك الذي ينادي بالتعامل القانوني الجديد مع شبكة الإنترنت، إذ إنه من خلال خصائص شبكة الإنترنت ذاتها نجد مقدمات لهذا الاتجاه، ذلك أن سهولة تطوير شبكة الإنترنت يعد منطقا تجديديًا كبيرًا يلزم المتعامل بها مواكبته[1].

ثالثا: الاتجاه الراجح في التعامل مع شبكة الإنترنت:

ما بين الاتجاه التقليدي في التعامل القانوني مع شبكة الإنترنت، وبين الاتجاه المطالب بالتعامل الجديد مع هذه الظاهرة، نجد أن الأمور تتخذ في الواقع اتجاهًا جديدًا لم يكن في الحسبان، ذلك أننا أمام ظاهرة وجدت في الخيال العلمي قديمًا، إلا أنها لم تتخط حاجز الخيال العلمي آنذاك، فقبل شبكة الإنترنت وثورة تكنولوجيا المعلومات وغيرها من الظواهر العلمية الجديدة كان العقل الإنساني يجعل منها نظرة خيالية بحيث لم تكن تشغله، أما اليوم فإن العقل البشري قد انتقل إلى مرحلة الانشغال بالظاهرة التي وجدت في الخيال العلمي قديمًا، بحيث أصبح مطلوبًا منه أن يرتقي بالمعلومة لكي يصبح لها مدلول وقيمة تتفق مع الجانب الاقتصادي.

وفي عملية الصراع ما بين التقليدي وبين الجديد في إطار شبكة الإنترنت تتساوى جميع الشعوب والدول، حتى الدول التي أخذت خطوات

(1) مصطفى السيد، دليلك إلى شبكة الإنترنت، دار الكتب العلمية، 2000، ص 15.

قانونية في هذا الشأن لم تضع جديدًا يذكر، وإنما حاولت في أطر نظمها التقليدية التجديد في مظاهر تعاملها مع الظاهرة الجديدة في محاولة لإبراز صلاحية نظمها القانونية.

والحقيقة أن اتجاهات التعامل التقليدي لن يكتب لها النجاح ما لم تتجه إلى التطوير بإصدار تشريعات خاصة، فتلك المحاولات وإن كانت تستمد معالمها من نظم قانونية عريقة إلا أنها لم تضع حلولا تتناسب مع قيمة الحدث العلمي للإنترنت، إذ انتهت تلك الحلول ولم تنجُ حتى من النقد الذاتي المتمثل في التعديل التشريعي المتوالي المنصب عليها، مثلما هو الحال في التشريع الأمريكي الذي لم يستقر على حال، بل إن الأحكام القضائية نجدها تشير صراحة إلى تعارضها مع الحقوق والحريات الأساسية مثلما هو الحال في القسم **1030** من الفصل **(18)** من التقنين الأمريكي (8 Sec 1030 USC) وهي المادة التي لحقها التعديل تلو التعديل منذ العام **1984** (وحتى تعديل **26 / 10 / 2001** الأخير)[(1)].

---

(1) § 1030. Fraud and Related Activity in Connection with Computers

(a) Whoever

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same

and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains،

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any one،year period;

(5)

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

مع الأخذ في الاعتبار النصوص الجديدة التالية المؤرخة عام 2002:

Provisions of Section 225 ("The Cyber Security Enhancement Act") and Section 896 of the Homeland Security Act of 2002, H.R. 5710 That Amend Title 18 of the United States Code, AMENDMENTS & REDLINE SHOWING CHANGES RESULTING FROM SECTION 896 OF THE 2002 HOMELAND SECURITY ACT AND SECTION SEC. 225 OF THE 2002 CYBER SECURITY ENHANCEMENT ACT:

- Title 18, Section 1030, Fraud and related activity in connection with computers
- Title 18, Section 2511, Interception and disclosure of wire, oral, or electronic communications prohibited
- Title 18, Section 2512, Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited
- Title 18, Section 2517, Authorization for disclosure and use of intercepted wire, oral, or electronic communications
- Title 18, Section 2520, Recovery of civil damages authorized
- Title 18, Section 2701, Unlawful access to stored communications
- Title 18, Section 2702, Voluntary disclosure of customer communications or records
- Title 18, Section 2703, Required disclosure of customer communications or records
- Title 18, Section 3125 Emergency pen register and trap and trace device installation

http://www.cybercrime.gov/homeland_225.htm

SEC. 225. CYBER SECURITY ENHANCEMENT ACT OF 2002

(a) SHORT TITLE.—This section may be cited as the "Cyber Security Enhancement Act of 2002".

(b) AMENDMENT OF SENTENCING GUIDELINES RELATING TO CERTAIN COMPUTER CRIMES.—

(1) DIRECTIVE TO THE UNITED STATES SENTENCING COMMISSION.— Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this subsection, the United States Sentencing Commission shall review and, if appropriate, amend its guidelines and its policy statements applicable to persons convicted of an offense under section 1030 of title 18, United States Code.

(2) REQUIREMENTS.—In carrying out this subsection, the Sentencing Commission shall— (A) ensure that the sentencing guidelines and policy statements reflect the serious nature of the offenses described in paragraph (1), the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses;

(B) consider the following factors and the extent to which the guidelines may or may not account for them—

(i) the potential and actual loss resulting from the offense;

(ii) the level of sophistication and planning involved in the offense;

(iii) whether the offense was committed for purposes of commercial advantage or private financial benefit;

(iv) whether the defendant acted with malicious intent to cause harm in committing the offense;

(v) the extent to which the offense violated the privacy rights of individuals harmed;

(vi) whether the offense involved a computer used by the government in furtherance of national defense, national security, or the administration of justice;

(vii) whether the violation was intended to or had the effect of significantlyinterfering with or disrupting a critical infrastructure; and

(viii) whether the violation was intended to or had the effect of creating a threat to public health or safety, or injury to any person;

(C) assure reasonable consistency with other relevant directives and with other sentencing guidelines;

(D) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(E) make any necessary conforming changes to the sentencing guidelines; and

(F) assure that the guidelines adequately meet the purposes of sentencing as set forth in section 3553(a)(2) of title 18, United States Code.

(c) STUDY AND REPORT ON COMPUTER CRIMES.— Not later than May 1, 2003, the United States Sentencing Commission shall submit a brief report to Congress that explains any actions taken by the Sentencing Commission in response to this section and includes any recommendations the Commission may have regarding statutory penalties for offenses under section 1030 of title 18, United States Code.

(d) EMERGENCY DISCLOSURE EXCEPTION.—

(1) IN GENERAL.—Section 2702(b) of title 18, United States Code, is amended—

(A) in paragraph (5), by striking "or" at the end;

(B) in paragraph (6)(A), by inserting "or" at the end;

(C) by striking paragraph (6)(C); and

(D) by adding at the end the following: "(7) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.".

(2) REPORTING OF DISCLOSURES.—A government entity that receives a disclosure under section 2702(b) of title 18, United States Code, shall file, not later than 90 days after such disclosure, a report to the Attorney General stating the paragraph of that section under which the disclosure was made, the date of the disclosure, the entity to which the disclosure was made, the number of customers or subscribers to whom the information disclosed pertained, and the number of communications, if any, that were disclosed. The Attorney General shall publish all such reports into a single report to be submitted to Congress 1 year after the date of enactment of this Act.

(e) GOOD FAITH EXCEPTION.—Section 2520(d)(3) of title 18, United States Code, is amended by inserting "or 2511(2)(i)" after "2511(3)".

(f) INTERNET ADVERTISING OF ILLEGAL DEVICES.— Section 2512(1)(c) of title 18, United States Code, is amended—

(1) by inserting "or disseminates by electronic means" after "or

other publication"; and

(2) by inserting "knowing the content of the advertisement and" before "knowing or having reason to know".

(g) STRENGTHENING PENALTIES.—Section 1030(c) of title 18, United States Code, is amended—

(1) by striking "and" at the end of paragraph (3);

(2) in each of subparagraphs (A) and (C) of paragraph (4), by inserting "except as provided in paragraph (5)," before "a fine under this title";

(3) in paragraph (4)(C), by striking the period at the end and inserting "; and"; and

(4) by adding at the end the following:

"(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

"(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.".

(h) PROVIDER ASSISTANCE.—

(1) SECTION 2703.—Section 2703(e) of title 18, United States Code, is amended by inserting ", statutory authorization" after "subpoena".

(2) SECTION 2511.—Section 2511(2)(a)(ii) of title 18, United States Code, is amended by inserting ", statutory authorization," after "court order" the last place it appears.

(i) EMERGENCIES.—Section 3125(a)(1) of title 18, United States Code, is amended—

(1) in subparagraph (A), by striking "or" at the end;

(2) in subparagraph (B), by striking the comma at the end and inserting a semicolon; and

(3) by adding at the end the following:

"(C) an immediate threat to a national security interest; or

"(D) an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year;".

http://www.cybercrime.gov/homeland_CSEA.htm

إن ذلك كله يقود إلى ضرورة بروز اتجاهات جديدة في التعامل القانوني مع شبكة الإنترنت، وهذه الاتجاهات الجديدة لن يكتب لها الاستمرار في مسايرة التطورات المتلاحقة في مجال قانون الإنترنت ما لم يكن هناك فهم قانوني سليم لعمل هذه التقنية وأهمية التنظيم القانوني لها, بل إن هذا المجال يوحي بجدارة الموضوع في القانون المقارن اجتهاد علماء القانون في توظيف النظرية وتطويرها لإيجاد الحلول القانونية القادرة على استيعاب هذه الظاهرة المتطورة بمزيد من التجديد والتطوير[1].

المطلب الثالث

خصائص قانون الإنترنت ومراتبه

يتميز قانون الإنترنت بمجموعة من الخصائص التي يجب أن نأخذها في الاعتبار عند رصد عملية التنظيم القانوني للإنترنت وهي: المنهجية، والقابلية للتطور، والتقنية.

كما يلزم الأخذ في الاعتبار عند البحث في قانون الإنترنت المراتب الثلاثة التي يتكون منها والتي يؤسس عليها الفقه النتائج في دراسة قانون الإنترنت، وسوف نعرض الخصائص في الفرع الأول، ثم نعرض المراتب في الفرع الثاني.

الفرع الأول

خصائص قانون الإنترنت

وهي تلك السمات التي تميز قانون الإنترنت كظاهرة تقنية - إنسانية

(1) الوثيقة العربية لقانون الإنترنت، المؤتمر الدولي الأول لقانون الإنترنت الغردقة 21: 25 أغسطس 2005. وفي المعنى ذاته: د. عمر محمد أبو بكر بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مرجع سابق، ص90.

تقوم على أرقى ما تم التوصل إليه من الناحية التقنية فيما يطلق عليه ثورة العلماء ومن ناتج الفكر الإنساني من المعلومات المحملة على الشبكة فيما يعرف بالمعلوماتية وتقوم على التواصل بين الشبكات وتسمح لأعداد غير محدودة باستخدام أقسامها الثلاثة في آن واحد، وهذه الخصائص هي المنهجية، والقابلية للتطور، والتقنية كمصدر من مصادره.

أولا: المنهجية:

يفسر مصطلح المنهجية في هذا المقام بمعناه التقليدي، وهو إمكان القيام ببناء منهجي للتنظيم القانوني للإنترنت يصلح لتقرير أحكام تأخذ بالنظرة التجديدية في نظرية القانون السائد، وذلك بإعادة تفسير تلك النصوص التقليدية لكي نضع أحكامًا في المنازعات التي تنشأ عن تلك المسائل، مع أن مسألة إعادة تفسير النصوص القائمة هذه يمكن أن تكون محل إعادة نظر دائمًا، ولكن يمكن الإقرار بها من حيث المشروعية لحين رصد معالم تفكير منهجي جديد يمكن أن يكون مستوحًى من رؤية جديدة، حيث إن العديد من المسائل التي تثار حين استخدام شبكة الإنترنت والتعامل بها لا يمكن أن تحكم بتفسير النصوص القائمة، وهنا يستعين القضاء المقارن بفلسفة جديدة تكون هي الدافع الأساسي لتوجيه المشرع إلى البحث عن حلول للمسألة سواء بتقرير التجديد أو التعديل على السواء.

فعلى سبيل المثال لا الحصر مسائل الاختصاص القضائي في المنازعات التي تنشأ عن استخدام شبكة الإنترنت، يمكن الاستعانة بشأنها بنظريات لها مكانتها في هذا الإطار، كما يمكن أن تكون هناك رؤية جديدة في هذا الشأن يقودها القضاء وفقًا لقاعدة جديدة تتصدى لذلك الفهم الذي ظل سائدًا لمرحلة طويلة من الزمن من أن تحديد الاختصاص يملكه المشرع أصالة وليس القاضي، وإرساء قاعدة جديدة تجعل "الاختصاص هو من عمل

القاضي وليس المشرع"، حيث نشأت في كنف القضاء المقارن فكرة جديدة هي فكرة المواقع الإيجابية والسلبية التي قد تحل محل فكرة اختصاص القضاء الوطني بنظر المنازعات والأفعال غير المشروعة التي تنشأ عن استخدام شبكة الإنترنت[1]، وهذه الفكرة تفيد في بناء منهجية جديدة في قواعد الاختصاص.[2]

(1) http://www.juriscom.net/chr/1/fr19980710.htm

(2) ظهرت هذه الفكرة في حكم للدائرة الاستئنافية الفيدرالية السادسة في الولايات المتحدة الأمريكية (CompuServe Inc. v. Patterson, 89 F. 3D 1257 6th cir. 1996) حيث قررت المحكمة في أسباب حكمها أن العالم اليوم يرتبط ببعضه بارتباط إلكتروني يتطور بحيث يجعل الاتصالات أسهل بصرف النظر عن بعد المسافة، وفي إشارة إلى اختصاص ولاية أوهايو (Ohio) استنادا إلى مصالح الولاية فيما يعرف بمبدأ (Long Arm Principal) لمباشرة الاختصاص القضائي على كل من هو غير مقيم في الولاية وهو مبدأ دستوري يتوافق مع الدستور الفيدرالي, وقررت المحكمة توافق العناصر الثلاثة للمبدأ من حيث وجود غرض المنفعة, وواقعة مرتكبة من قبل من هو غير مقيم في الولاية، وأخيرا أن تأكيد الاختصاص عادل.

ولقد وجدت المحكمة كل هذه الأمور متوافرة, ولقد كان محتوى السؤال هنا: هل كان المدعى عليه يسعى إلى تحقيق منفعة لنفسه من القيام بعمل في نطاق الولاية (وهذا هو صلب الاختصاص هنا) حيث يجب على غير المقيم في الولاية القيام باتصال رئيسي مع الولاية يجعله عرضة للتقاضي فيها، ومثل هذا الأمر لا يتطلب وجوده ماديا في الولاية، ولقد وجدت المحكمة أن (Patterson) قد أحدث اتصالا رئيسيا (Substantial Connection) بالولاية يبرر اختصاص قضائها, حيث إنه دخل في عقد يسمح بتطبيق قانون أوهايو وذلك بالتعاقد مع (CompuServe) لعدة سنوات, وكذلك قيامه بإرسال برمجيته لكي يتم تخزينها وبالتالي تسويقها من خلال خوادم (CompuServe) في ولاية أوهايو, وباجتماع هذه العناصر يتبين أن (Patterson) يبدو وكأنه يعمل في ولاية أوهايو (Ohio) على الرغم من وجوده المادي في تكساس (taxas). حول تفاصيل هذه القضية راجع: =

= مجموعة من الخبراء، المعاملات الرقمية وقانون الإنترنت، المنظمة العربية للتنمية الإدارية، 2006، ص 159.

ومن التطبيقات القضائية في دولة الإمارات العربية المتحدة ما حدث في إمارة دبي عندما تفاجأت إحدى ملكات الجمال السابقات أثناء وجودها بدبي بوجود خبر على أحد مواقع شبكة الإنترنت مفاده سريان شائعات عن وفاة ثري عربي خلال ممارسة الجنس معها، الأمر الذي حدا بها إلى التقدم ببلاغ للنيابة العامة، وبعد التحقيق أسندت النيابة العامة للمتهم صاحب هذا الموقع أنه أسند بطريق النشر بموقع صحيفة على شبكة الإنترنت الواقعة الواردة بالتحقيقات والماسة بعرضها على النحو الذي يجعلها محلا للازدراء والعقاب، وطالبت عقابه بالمادتين [3/9، 372] من قانون العقوبات الاتحادي رقم 3 لسنة 1987.

وبتاريخ 2003/4/16 قضت محكمة أول درجة غيابيا بعدم اختصاص محكمة دبي بنظر الدعوى على اعتبار أن موقع شبكة الإنترنت مصدره لندن، وأن الخبر تم نشره من هناك، وأن إقامة المتهم بلندن أيضا، كما قضت المحكمة بعدم قبول الدعوى المدنية وألزمت رافعها بالمصروفات.

وطعنت النيابة العامة على الحكم السابق بالاستئناف طالبة إلغاء الحكم المستأنف وإدانة المتهم، كما طعن وكيل المدعية بالحق المدني بالاستئناف، وبجلسة 2003/6/11 قضت محكمة الاستئناف بقبول الاستئنافين شكلا وفي الموضوع بإلغاء الحكم المستأنف بشقيه وإعادة القضية إلى محكمة أول درجة للفصل في موضوعها، وأسست محكمة الاستئناف قضاءها على أن المادة [2/16] من قانون العقوبات الاتحادي نصت على أنه: [تعتبر الجريمة مرتكبة في إقليم الدولة إذا وقع منها فعل من الأفعال المكونة لها، أو إذا تحققت فيها نتيجتها، أو كان يراد أن تتحقق فيها]، ولما كان ذلك وكان الثابت من الأوراق أن الواقعة محل الاتهام تم نشرها بموقع [...] على شبكة الإنترنت، وأن المجني عليها حين اطلاعها على الموقع أثناء وجودها بدبي طالعت الخبر محل الاتهام، ومن ثم تكون نتيجة الفعل قد تحققت في إمارة دبي، وتعتبر الجريمة إذا ما استوفت باقي أركانها قد وقعت في إقليم الدولة وتخضع لأحكام قانون العقوبات الاتحادي رقم [3] لسنة 1987، ومن ثم تقضي المحكمة بإلغاء الحكم المستأنف والقضاء باختصاص محكمة دبي الابتدائية وانتهت إلى حكمها السابق ذكره، وبجلسة 27/ 7/ 2003 قضت =

ثانيًا: القابلية للتطور:

يقصد بهذا المصطلح - باعتباره من خصائص التنظيم القانوني للإنترنت - أن المرحلة المعاصرة تعد مرحلة بناء، تستوعب حركة فرع جديد من فروع القانون على مستوى سن التشريع وعملية تفسير القضاء له، ويمكن ملاحظة أمرين في هذا الإطار، الأمر الأول: منطق تفاعل التقنية مع مصادر القانون التقليدية، والأمر الثاني: نشأة اتجاه مدرسي جديد يتناول بالتفسير مراتب شبكة الإنترنت كمعيار يتم الاستناد إليه للحصول على تفسيرات منطقية لفلسفة التنظيم القانوني للإنترنت.

ثالثًا: التقنية من مصادر قانون الإنترنت:

يعرف المصدر بأنه الواقعة المنشئة للالتزام، وتتعدد المصادر فهي في القانون المدني خمسة وإن اختلفت في ترتيبها فيما بين القوانين العربية، وهي الشريعة الإسلامية والتشريع والعرف وقواعد القانون الطبيعي ومبادئ العدالة، وإزاء ثورة تكنولوجيا المعلومات والاتصالات نشأ اتجاه في الفقه المقارن يعرض لمنطق إمكانية إضافة التقنية أو التكنولوجيا إلى تلك المصادر. وفي هذا اختلفت الرؤية ما بين التقرير بإضافة التقنية كمصدر مستقل أو إضافتها إلى القانون الطبيعي باعتبار أن التقنية هي القانون

= المحكمة الابتدائية غيابيا بمعاقبة المتهم بالحبس لمدة ثلاثة أشهر عما نسب إليه من اتهام، وفي الدعوى المدنية بإحالتها إلى المحكمة المدنية المختصة.
هذا الحكم وبالرغم من أنه قام بتطبيق نصوص قانون العقوبات التقليدية والقائمة بخصوص جريمة القذف الواقعة عن طريق شبكة الإنترنت، إلا أنه وضع حدا للقول بعدم تطبيق القوانين الوطنية على الجرائم الواقعة بالإنترنت إذا ارتكبت خارج إقليم الدولة. القضية رقم [2002/5234] جزاء دبي، واستئنافاها رقما [1248، 2003/1252] جزاء دبي.

الطبيعي للتعامل عبر شبكة الإنترنت.

وتعد التقنية أساس العمل في نظام شبكة الإنترنت، وهي مصدر لازم لا يمكن الاستغناء عنه، بل إنها هي التي أتت بشبكة الإنترنت، والتقنية بهذا المفهوم هي وليدة نشاط علمي وتتمثل في التطبيق العملي للحركة العلمية النظرية، فهي بهذا المعنى جزء من العلم وليست بعيدة عنه، فبدون التقنية يضحى العلم مجرد نظريات غير ذات جدوى[1].

وقد أسست التقنية لتقسيم شبكة الإنترنت إلى أقسام ثلاثة، وسمحت بإطلاق إمكانيات تطويرها، وقد ساعد على ذلك روح المنافسة الحرة بين العلماء، حتى إنه يمكن أن يقال: إن تقنية شبكة الإنترنت أرقى وأعظم سوق حرة في العالم، وهي تعد حصيلة الثقافة والحضارة، وبهذا المعنى يمكننا القول بأن التقنية تخلق المعلوماتية.

الفرع الثاني

مراتب شبكة الإنترنت Internet Layers

الأصل أن شبكة الإنترنت غير مملوكة لأحد, ولكن الواقع يقول إن ملكية شبكة الإنترنت مقسمة بين الدول والحكومات والجامعات والشركات والمؤسسات، أما من يملك الخدمات الرئيسية للإنترنت فهو مقدم خدمة شبكة الإنترنت ISP (Internet Server Provider) وتقع عليه مسئولية قانونية سواء تقصيرية أو تعاقدية، أو جنائية في بعض الأحيان.

وتدار شبكة الإنترنت عن طريق عدة هيئات، ففي المستوى الأعلى يوجد عدد من الهيئات التنظيمية مسئولة عن تكنولوجيا وهندسة شبكة

(1) الوثيقة العربية لقانون الإنترنت الصادرة عن المؤتمر الدولي الأول لقانون الإنترنت الغردقة 21: 25 أغسطس 2005.

الإنترنت، مثل مؤسسة بناء شبكة الإنترنت، وتتضمن فريق العمل الذي يتكون من مصممي الشبكة والقائمين على تشغيلها والباحثين والمهتمين بتطويرها.

كما توجد أيضًا شركات شبكة الإنترنت المكلفة بتسجيل أسماء النطاق Domain name بالأسماء والأرقام ICANN **Internet Corporation for Assigned Names and Numbers** وهي شركات لا تهدف إلى الربح، ومهمتها تحديد نظام إدارة أسماء ملاك مواقع شبكة الإنترنت.

كما يوجد اتحاد لتنمية المعاهدات الدولية وتطوير شبكة الإنترنت، أطلق عليه "اتحاد شبكة الإنترنت" ومقره في جنيف بسويسرا **World Wide Web Consortium- W3C-**، وهو عبارة عن اتحاد دولي أنشئ من أجل تطوير وتعديل المعاهدات الدولية بما يتناسب وتطور تكنولوجيا شبكة الإنترنت، وهذه الهيئات تتعاون فيما بينها من أجل إدارة تلك الشبكة.

الحديث عن مراتب شبكة الإنترنت هو حديث فني متخصص جدًا، ولكن ينبغي علينا نحن كقانونيين أن نكون ملمين ولو بشيء يسير عن طريقة عمل هذه التقنية، كما أن المشتغلين بالجوانب القانونية المتصلة بهذا المجال من رجال أمن ووكلاء نيابة وقضاة ومحامين يجب عليهم المعرفة بهذه التقنية وخاصة في كيفية وقوع الجريمة وكيفية التعامل مع الدليل الرقمي.

الأصل أن للإنترنت مراتب ثلاثة هي على التوالي: مرتبة القطع الصلبة dwere LayerHar والقطع المرنة المنطقية ic LayerLog ومرتبة المحتوى Content Layer،[1] فكل من هذه المراتب يعمل الفقه على تأسيسها والاستناد إليها في البحث في قانون الإنترنت انطلاقًا من بحث نقاط

(1) www.cyberlaw.org.ly

القانون الطبيعي ومصادر القانون عبر شـبكة الإنترنـت، وتصـلح مراتـب شـبكة الإنترنـت لوضـع منطق التفاعل مع أقسامه، فهذا التقسيم يتيح في الحقيقة وضع أقسـام قـانون الإنترنـت موضـع التنفيذ الفعلي، على أن الأمر لم يقـف عنـد الأصـل المـذكور فقـد تطـورت النظـرة إلى طبقـات أو مراتب شبكة الإنترنت لكي تصل إلى ست مراتب، إذ بالنظر إلى شـبكة الإنترنـت كنظـام اتصـالات بين مستخدميها يمكن القول بأن هناك ست مراتب تتشكل منها شبكة الإنترنت، وهي:

- مرتبة المحتوى: وهي الرموز والصور التي تتواصل فيما بينها.
- مرتبة التنفيذ: البرامج التي تستخدمها شبكة الإنترنت، مثل الويب.
- مرتبة الناقلة: بروتوكول TCP الذي يقوم بتقسيم البيانات إلى حزم.
- مرتبة بروتوكول شبكة الإنترنت: فيما يعـرف ببروتوكـول شـبكة الإنترنـت IP الـذي يتـولى تدفق البيانات عبر الشبكة.
- مرتبة الرابط: الواجهة بين مستخدمي الحاسوب وفيزياء الطبقة.
- مرتبة الفيزياء أو الطبقة الماديـة: السـلك النحـاسي أو الكابـل البصري أو روابـط الأقـمار الصناعية...الخ.[1]

---

(1) What are the layers of the Internet? Viewed as a system of communication between users، the six layers that constitute the Internet are:

- The Content Layer—the symbols and images that are communicated.
- The Application Layer—the programs that use the Internet، e.g. the Web.
- The Transport Layer—TCP، which breaks the data into packets.
- The Internet Protocol Layer—IP، handles the flow of data over the network.
- The Link Layer—the interface between users' computers and the physical layer.

ولما كانت شبكة الإنترنت هي أداة أو صلة بين الشبكات دون اعتبار للحدود الدولية فهي تعد مظهرًا للتطور الحادث في تكنولوجيا المعلومات، ومكمنًا للإبداع الكامن في تلك الثورة[1]، ويكمن الإبداع في شبكة الإنترنت في أنه لم يحدث مصادفة وإنما حدث بسبب هيكلتها، حيث تعد هذه الهيكلة من توليفة من المراتب Layers التي يطلق عليها شفرات Code، كما أنها تُعرف بمفهوم المكونات الوظيفية في نظم الاتصالات Functional components of a communications system.

ولكن ما هي مراتب شبكة الإنترنت بشكل عام؟ في أثناء إعداد برنامج حاسوب فإن إعداد مراتبه يعني تنظيم البرمجة وتقسيمها إلى عناصر وظيفية منفصلة يمكنها أن تتفاعل بطريق تسلسلي أو هرمي، حيث يكون لكل مرتبة في العادة واجهة للمرتبة العليا التي تعلوها ولتلك التي أسفلها، ويتم إعداد برامج الاتصالات غالبًا في شكل مراتب، والمثال على ذلك هو بروتوكول TCP/IP[2]، الذي

- The Physical Layer—the copper wire، optical cable، satellite links، etc.

  See: Lawrence B. Solum and Minn Chung، The Layers Principle: Internet Architecture and the Law، University of San Diego School of Law، Public Law and Legal Theory Research Paper 55

  June 2003، This paper can be downloaded without charge from the Social Science Research Network Electronic Paper Collection: http://ssrn.com/abstract=416263

(1) Lawrence Lessig، The Future of Ideas: the Fate of the Commons in a Connected World 5-23 (Random House 2001). www.Amazon.com

(2) TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network

(either an intranet or an extranet). When you are set up with direct access to the Internet، your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP. TCP/IP is a two،layer program. The higher layer، Transmission Control Protocol، manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer، Internet Protocol، handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others، they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point،to،point، meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher،level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

Many Internet users are familiar with the even higher layer application protocols that use TCP/IP to get to the Internet. These include the World Wide Web's Hypertext Transfer Protocol (HTTP)، the File Transfer Protocol (FTP)، Telnet (Telnet) which lets you logon to remote computers، and the Simple Mail Transfer Protocol (SMTP). These and other protocols are often packaged together with TCP/IP as a "suite."

يتكون من مرتبتين رئيسيتين الأولى هي: TCP[1] والثانية هي:

Personal computer users with an analog phone modem connection to the Internet usually get to the Internet through the Serial Line Internet Protocol (SLIP) or the Point،to،Point Protocol (PPP). These protocols encapsulate the IP packets so that they can be sent over the dial،up phone connection to an access provider's modem.

Protocols related to TCP/IP include the User Datagram Protocol (UDP)، which is used instead of TCP for special purposes. Other protocols are used by network host computers for exchanging router information. These include the Internet Control Message Protocol (ICMP)، the Interior Gateway Protocol (IGP)، the Exterior Gateway Protocol (EGP)، and the Border Gateway Protocol (BGP).

(1) TCP (Transmission Control Protocol) is a set of rules (p2otocol)' used along 7ith the Internet Protocol (|ahref=http://searchNetworking.techtarget.com/sDefinition/0،sid7_gci214031،00.html class=inline>IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data، TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

For example، when an HTML file is sent to you from a Web server، the Transmission Control Protocol (TCP) program layer in that server divides the file into one or more packets، numbers the packets، and then forwards them individually to the IP program layer. Although each packet has the same destination IP address، it may get routed differently through the network. At the other end (the client program in your computer)، TCP reassembles the individual packets and waits until they have arrived to forward them to you as a single file.

TCP is known as a connection،oriented protocol، which means that a

IP[1] حيث يتشكل من تجمع برامج تسمح بنقل وإعداد وظائف عنوان

---

connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model، TCP is in layer 4، the Transport Layer.

1) The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example، an e،mail note or a Web page)، the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

Because a message is divided into a number of packets، each packet can، if necessary، be sent by a different route across the Internet. Packets can arrive in a different order than the order they were sent in. The Internet Protocol just delivers them. It's up to another protocol، the Transmission Control Protocol (TCP) to put them back in the right order.

IP is a connectionless protocol، which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right

الشبكة في اتصالات شبكة الإنترنت، ويطلق على هاتين المرتبتين TCP/IP وبعض مراتب البرامج الأخرى عبارة Protocol stack.

ويتم ترتيب الطبقة في شكل عمودي، وعندما يتم الاتصال عبر شبكة الإنترنت بالمعلومات فإنها تتدفق من طبقة المحتوى (أعلى مستوى) عبر طبقة التنفيذ، ثم الطبقة الناقلة، ثم طبقة بروتوكول شبكة الإنترنت، ثم طبقة الرابط، ثم الطبقة المادية (وهذه الأخيرة أدنى مستوى)، حيث تعبُر الطبقة المادية في حزم، ومن ثم تتدفق عائدة من خلال الطبقات ذاتها إلى مصدر الأمر.

ويتطلب الاتصال عبر شبكة الإنترنت أن يكون المحتوى رقميًا باستعمال الطبقة، ومن ثم فإن المعلومات الرقمية يتم تجزئتها إلى حزم من قِبل الطبقة الناقلة، ويتم توجيهها من قِبل طبقة بروتوكول شبكة الإنترنت، حيث يمكنها المرور باستخدام طبقة الرابط إلى الطبقة المادية، فإذا وصلت المعلومات إلى الطبقة الدنيا فإنها تتحرك أفقيا، وتقوم الطبقة المادية بإرسال واستقبال حزم بيانات فردية باستخدام سلك نحاسي أو ألياف بصرية أو راديو من خلال نقاط مختلفة إلى نقطة نهائية أو الوجهة المقصودة عبر الشبكة، فإذا وصلت إلى وجهتها المقصودة تبدأ البيانات في الصعود عموديًا

---

order is because of TCP، the connection،oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model، IP is in layer 3، the Networking Layer.

The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However، IP Version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

عبر الطبقات لكي يتم تفسيرها باستعمال طبقة المحتوى، وذلك كله يؤدي إلى القول بأن هيكلة شبكة الإنترنت ككل عبارة عن طبقات[1].

وللتحقيق في الجرائم الناشئة عن الإنترنت يتطلب الأمر جمع الأدلة لإثبات وقوع الجريمة، كما يتطلب تعيين هوية الشخص أو الأشخاص المسئولين عن هذه الجريمة، ولهذا الغرض يمكن احتجاز البيانات المتنقلة في المسارات, حيث يتم إرسال كافة البيانات في صورة حزم، ويحدد في كل حزمة المرسل والمرسل إليه في حقول محددة داخلها، ويتم تقديم هذه البيانات بالشكل المحدد في خدمة نظام اسم النطاق (DNS)، والمعروف باسم "عناوين بروتوكولات الإنترنت IP. وتُوجه الحزم عبر الإنترنت من الخادم القائم بإرسال هذه الحزم، ثم تسير عبر خوادم وسيطة حتى تصل إلى جهة الوصول، وتُخزن البيانات المتنقلة عبر المسارات طوال الفترة اللازمة للتأكد من إتمام الاتصال بنجاح، وقد يقوم الخادم القائم بإرسال هذه الحزم بحجز البيانات لفترة أطول بهدف ترتيب مواقع الأسماء، أو لأسباب فنية أو قانونية أخرى، مما يتسبب في حجز البيانات المتنقلة عبر المسارات، وقد طبق الاتحاد الأوروبي تعليمات احتجاز البيانات[2] التي تتطلب من الدول

---

(1) الوثيقة العربية لقانون الإنترنت الصادرة عن المؤتمر الدولي الأول لقانون الإنترنت الغردقة، 21: 25 أغسطس 2005.

تحتوي كل طبقة على مجموعة من القواعد والبروتوكولات التي تقدمها للطبقات التي تليها, ومن الجدير بالذكر أنك لا تشعر بأي طبقة من تلك الطبقات, وإنما فقط نلاحظ الطبقة التي تظهر فيها البرامج التي يتم استخدامها، لمزيد من التفاصيل يراجع الموقع الإلكتروني: www.wikipedia.org

(2) تعليمات رقم 2006/24/EC التي أصدرها البرلمان الأوروبي للمجلس في 15 مارس 2006 بشأن احتجاز البيانات الصادرة أو التي تمت معالجتها بصدد توفير خدمات اتصال إلكترونية متوافرة لعامة الجماهير أو الخاصة بشبكات الاتصال=

الأعضاء في الاتحاد الأوروبي أن تفرض شرطًا أساسيًا ضمن تشريعاتها القومية على مُشغلي الاتصالات عن بعد، وهو حجز البيانات المتنقلة عبر المسارات لمدة ستة أشهر على الأقل، وعامين على الأكثر، ويعمل عنوان البروتوكول على التعرف على جهاز الكمبيوتر الذي أُرسلت منه هذه الحزمة، وبالتالي يتم التعرف على الشخص المستخدم لهذا الجهاز، غير أن التعرف على الشخص المستخدم لن يكون ممكنًا إذا كان جهاز الكمبيوتر متاحًا لعدد من المستخدمين، كما هو الحال في مقاهي الإنترنت، التي لا تحتفظ بسجلات تحدد مستخدمي الأجهزة وأوقات الاستخدام.

هذا فضلا عن خدمات إعادة الإرسال المجهولة المصدر، والخدمات الأخرى التي تزيل هوية المرسل الرئيسي من الحزمة، وتستبدل تلك الهوية بعنوان بروتوكول الإنترنت الخاص ببرنامج إعادة الإرسال، وبهذه الطريقة يمكن الوصول إلى رابط عنوان IP الرئيسي فقط من خلال خدمة إعادة الإرسال دون الوصول إلى شخص المرسل.

ويتم إرسال الحزم عبر الشبكة في هيئة سلسلة من الممارسات المتشابهة، وبخلاف البريد الإلكتروني التقليدي لا يفقد المرسل البيانات عند إرسالها إلى المرحلة التالية في سلسلة الاتصال، ويتم حفظ البيانات حتى يقضي البرنامج بحذفها، ويحدث ذلك عند تأكيد الاستلام الآمن، ورغم ذلك وسعيًا لتحسين حركة مسارات الشبكة بأفضل طريقة، يمكن إجراء تخزين مؤقت لكافة مجموعات الحزم التي تشكل المعلومات الأصلية في خادم الوكيل.

وبالإضافة إلى ذلك، عندما تقوم محركات البحث بفهرسة موقع إلكتروني، تُخزن المعلومات التي فهرستها (أي الموقع الإلكتروني) بصورة

= العامة، والمعدل لتعليمات رقم 2002/58/EC.

نموذجية في نظمها (وغالبًا تُحفظ بصورة مضللة في هيئة "الذاكرة المخبأة").

وبناء على ذلك، قد يتوافر موقع إلكتروني عن طريق خادم الوكيل، ويحتفظ النظام بذاكرة مخبأة من محرك البحث أو من نظم التخزين الأخرى حتى بعد إزالة المعلومات الأصلية من الموقع الإلكتروني الأصلي.

ويتبين من خلال ذلك أن مسرح تلك الجريمة يعد دوليًا، وأن الأدلة في الغالب قد تخضع لسلطة قضائية أخرى بخلاف هيئة تطبيق القانون التي تتولى إجراء التحريات، وبذلك يعد التعاون الدولي أمرًا بالغ الأهمية، وجدير بالذكر أن الاتفاقية الأوروبية لمكافحة الجريمة المعلوماتية[1] تمثل تقدمًا ملحوظًا في اتجاه تحقيق هذا التعاون الدولي.

المطلب الرابع

أقسام قانون الإنترنت

ينقسم قانون الإنترنت Cyberlaw والذي يتناول موضوعه "التنظيم القانوني للإنترنت" إلى خمسة أقسام كبرى نتناولها على النحو التالي:

القسم الأول: التخزين الرقمي Digital Storage:

القسم الثاني: قواعد البيانات Data Base:

القسم الثالث: المعاملات الرقمية Digital Transaction:

القسم الرابع: القانون الجنائي عبر شبكة الإنترنت Cybercrime:

القسم الخامس: التجارة الإلكترونية Electronic Commerce:

- القسم الأول: التخزين الرقمي **Digital Storage**:

حيث يتناول التنظيم القانوني لتخزين البيانات وطرائق القيام بها ووسائل

(1) http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

حمايتها.[1]

- القسم الثاني: قواعد البيانات **Data Base**:

وهو القسم الذي يتناول دراسة الأنماط المختلفة للتخزين في الوقت الذي يجب أن تتجاوب في هيكلتها التخزينية مع القيمة الاستردادية لها المثلة في المعلومة المحددة التي يستعرضها الباحث، وموضوع قواعد البيانات هذا من المشكلات التي تقابل الفكر الفلسفي الغربي دون العربي الذي يستند في جذوره الأولى إلى فلسفة الفكر الموسوعي منذ أن وضع أبو الفرج بن النديم في العراق "الفهرست" في القرن الرابع الهجري/ العاشر الميلادي[2] ليكون

---

(1) ظهر مفهوم التخزين الرقمي الدائم للمعلومات منذ بدايات ظهور الحاسبات الآلية, ومن خلال هذا المفهوم تطورت وحدات التخزين بصورة مذهلة عبر العقود السابقة, ولم يعد هناك الآن حاسب شخصي- أو خادم وكذلك الكاميرات والتليفونات وغيرها بدون وحدة تخزين أو أكثر تعمل بمفهوم التخزين الرقمي للمعلومات, أي تخزين المعلومات بطريقة تجعل من السهل استرجاعها في أي وقت.

http://forum.stop55.com/112298.html

(2) ابن النديم هو أبو الفرج محمد بن إسحاق بن محمد بن إسحاق توفي 17 سبتمبر عام 995م, وهو أديب وكاتب سيرة ومصنف وجامع فهارس عربي شيعي صاحب الكتاب المعروف بالفهرست، والذي جمع فيه كل ما صدر من الكتب والمقالات العربية في زمنه, لا يعرف الكثير عن حياته ولا سبب تكنيته بأبي النديم, عاش ببغداد وعمل كاتبا وخطاطا ونساخا للكتب وهي مهنة ورثها عن أبيه, تتلمذ على يد السيرافي وعلي بن هارون المنظم والفيلسوف أبي سليمان المنطقي, وانتسب إلى جماعة علي بن عيسى- وزير بني الجراح العارف بأصول المنطق وسائر علوم الإغريق والفرس والهنود كما فعل صاحبه الخطاط يحيى بن عدي، كما التقى في فترة من حياته بالفيلسوف المسيحي ابن الخمار، ولم يكن من بين شيوخه أبدا عالم من السنة، بل كان أغلبهم من عاشقي الفلسفة وخاصة فلسفة أرسطو, كتابه الرئيس كان كتاب الفهرست الذي نشره عام 938 والذي قال عنه في مقدمته: إنه جامع لكل ما صدر من الكتب العربية وغير العربية، وكان بذلك ابن النديم أول المصنِّفين =

بذلك أول موسوعي في التاريخ العالمي يضع منهجية أولية وأساسًا لفكر قواعد البيانات.

- القسم الثالث: المعاملات الرقمية **Digital Transaction**:

حيث يتناول هذا القسم حركة المعاملات المدنية المختلفة عبر شبكة الإنترنت، مثل موضوع الحقوق والحريات، والالتزامات الرقمية، والملكية الفكرية، والعقود الرقمية، وغيرها من الموضوعات ذات العلاقة.[1]

= في العالم، حيث لم يكن قبله إلا كتب تصنف الشعر والشعراء تسمى الطبقات. وكان هو من أدخل كلمة الفهرست الفارسية إلى العربية.

http://ar.wikipedia.org/wiki

وفي العصر الحديث وتحديدا في عام 1945 قدم أول تصور في هذا الخصوص من قبل الأمريكي Vanever Bush في مقالته As we may think، مستندا إلى منهج عمل أول سكرتيرة عملت في الحكومة الأمريكية وهي السيدة Francis Perkins، حيث أكد Bush على "أن الأسلوب الهجائي والرقمي في ترتيب الوثائق والمعلومات يُعد الوسيلة المثلى التي يمكن من خلالها الحصول على المعلومات" لذلك قدم تصوره في استحداث طريقة لاسترداد أو استرجاع المعلومات، أطلق عليها MEMEX واعتبرها كفيلة بتخزين البيانات من كتب وسجلات، ثم إنه يمكن استردادها على هيئة معلومات محددة كلما تطلب الأمر ذلك. ولم يمض عقد من الزمن حتى تفتقت الأذهان عن أهمية نظام استرداد البيانات المذكور، وتسارعت خطواته شيئا فشيئا حتى وصل بفضل تطور الوسائل التقنية إلى إمكانية تخزين واسترداد المعلومات في أي شكل كانت عليه ولو كانت في هيئة صوت وصورة عبر سلسلة التصغير الفيلمي والميكروفيلم وغيرها من الوسائل عن طريق استخدام التكنولوجيا. راجع حول ذلك: د. هيفاء أيوب ججاوي، الأسلوب العلمي في تقييم قواعد البيانات من وجهة نظر المكتبيين، المجلة العربية للمعلومات، المنظمة العربية للتربية والعلوم والثقافة، 2000، ص 22.

(1) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص10.

وهو أحد أقسام قانون الإنترنت الأكثر تجاوبًا مع الحاجات اليومية لمستخدمي شبكة الإنترنت وأعضاء شبكة الإنترنت عمومًا، فهو القسم الذي يمكن أن نطلق عليه لفظة القانون المدني عبر شبكة الإنترنت، حيث يحتوي على كافة ما يمكن أن ينسب إلى المعاملات المدنية وفق مفهوم العالم المادي، فهو في هذا يعد البوتقة التي تحتوي في داخلها على كافة مظاهر التعامل عبر شبكة الإنترنت من حقوق وحريات والتزامات رقمية وملكية فكرية وعقود رقمية عبر شبكة الإنترنت، والتي تمتاز بسرعة تطورها وتجددها واختلافها عما هي عليه في الحياة المادية.

- القسم الرابع: القانون الجنائي عبر شبكة الإنترنت **Cybercrime**:

ويشمل هذا القسم القاعدة الموضوعية والقاعدة الإجرائية على حد سواء، حيث يتناول في موضوعه رؤية الفقه والقضاء والمشرع لموضوع الحماية الجنائية التي تتم لكافة ما يتعلق بشبكة الإنترنت، ثم إن هذا القسم يتناول أيضًا البحث في التطوير الذي تتعرض له القاعدة الإجرائية اليوم مع ما يصاحب هذا الأمر من بروز الدليل الرقمي Digital Evidence[1] الذي يعد الشغل الشاغل في المرحلة المعاصرة لعلماء العدالة الجنائية.

- القسم الخامس: التجارة الإلكترونية **Electronic Commerce**:

وهذا القسم من أقسام قانون الإنترنت يتجاوب مع فكرة التجارة عبر شبكة الإنترنت بما في ذلك التطورات الحادثة فيها والتي صاحبها العديد من التفسيرات، ويشمل ذلك بالطبع استخدام شبكة الإنترنت في التجارة، أو

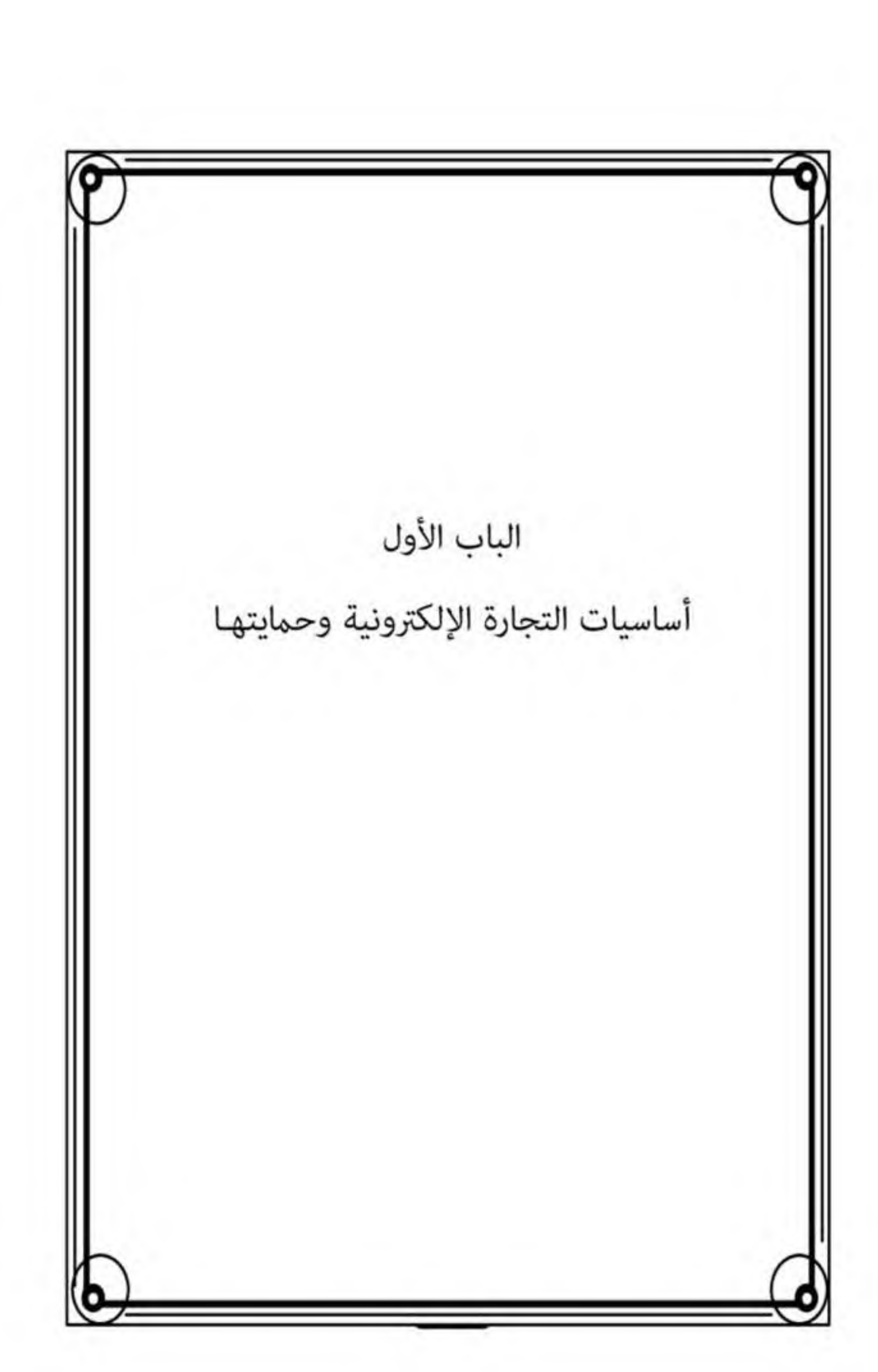
(1) عرف الدليل الرقمي بأنه: (بيانات يمكن إعدادها وتراسلها وتخزينها رقميا بحيث تمكن الحاسوب من تأدية مهمة ما) أو أنه (الدليل الذي يجد له أساسا في العالم الافتراضي). مشار إليه لدى د. عمر محمد أبو بكر بن يونس، الدليل الرقمي، الجمعية العربية لقانون الإنترنت، 2008، ص 25.

التجارة الرقمية عينها كما هو الشأن في الاتجار بمواد رقمية ليس لها وجود سوى في بيئة تكنولوجيا المعلومات مثل البرمجيات والبرامج وغيرها.[1]

وهذا القسم هو محل بحثنا في هذه الدراسة، وسوف نتناوله تفصيلا من خلال بيان أساسيات التجارة الإلكترونية وحمايتها والجرائم الواقعة عليها.



(1) الوثيقة العربية لقانون الإنترنت، المؤتمر الدولي الأول لقانون الإنترنت الغردقة، 21: 25 أغسطس 2005.



الباب الأول

أساسيات التجارة الإلكترونية وحمايتها

الباب الأول

أساسيات التجارة الإلكترونية وحمايتها

تمهيد وتقسيم:

مع التقدم الهائل والمتزايد في تكنولوجيا المعلومات والاتصالات Communication Information & Technologies ونمو شبكة الإنترنت ودخولها حيز الخدمة المدنية، وسهولة الدخول إليها والتعامل معها، وتخفيض نفقات الاشتراك فيها، ظهرت العديد من التطورات المهمة التي أثرت على عمليات التبادل التجاري، فحدثت تغيرات جذرية في أسس التبادل التجاري الدولي، وزاد حجم التجارة الدولية، وكان من أهم هذه التطورات ظهور التجارة الإلكترونية.

فالسلوك التجاري والاقتصادي للإنسان كان دائمًا وليد الحاجة والظروف، فالتاريخ الاقتصادي للبشرية ما هو إلا ردود أفعال لتلبية الاحتياجات المتغيرة واللانهائية للإنسان، فالنقود مثلا لم تنشأ بقرار أو بقانون، وإنما فرضتها الحاجة الإنسانية إلى مخزن للقيمة ووسيلة للتقويم بعد أن تطورت عملية المبادلة في التجارة واتسعت، ثم ظهرت بعد ذلك التشريعات والقوانين التي تنظم حركتها، وكذلك الحال بالنسبة للتجارة الإلكترونية فإنها لم تنشأ بقرار أو تشريع، بل ظهرت استجابة لمتطلبات السرعة في العملية التجارية، ثم ظهرت بعد ذلك القوانين المنظمة لها، فالوقت له قيمته في التجارة، وقد يؤدي التأخير في قبول صفقة إلى فوات ربح ضخم، كما أن الأسعار سريعة التقلب، والفوائد البنكية تتغير من يوم إلى آخر، الأمر الذي أدى إلى البحث عن طرق سريعة للتعاقد.

والتجارة الإلكترونية لم تظهر فجأة بل كانت وليدة المراحل المختلفة

التي مرت بها ثورة الاتصالات والمعلومات، ونموًا طبيعيًا لاستخدام الشبكات وتكنولوجيا المعلومات والاتصالات العالمية المتوفرة في العالم وخصوصًا شبكة الإنترنت، فانتشار شبكات نقل المعلومات بصورة واسعة النطاق لتربط ملايين الحاسبات الآلية على مستوى دول العالم في منظومة عملاقة من قواعد البيانات أدى بدوره إلى تلاشي الحدود الجغرافية بين الدول، وتحول العالم إلى قرية صغيرة، كل ذلك هيأ العالم للآليات الجديدة باستخدام الحواسب والشبكات الإلكترونية، حتى أصبحت الحاجة إلى التجارة الإلكترونية مطلبًا ضروريًا ومهمًا، ومن المتوقع أن تستحوذ التجارة الإلكترونية على 70% من حجم التجارة العالمية بحلول عام 2010، ولذلك يسود العالم الآن اهتمام متصاعد بالتجارة الإلكترونية باعتبارها أحد روافد ثورة المعلومات، ونتيجة مباشرة للتطورات التقنية في مجال الحاسب الآلي والمعلوماتية، ونتيجة غير مباشرة لاستخدام شبكة الإنترنت.

وبواسطة استخدام التجارة الإلكترونية يستطيع البائع الآن اتخاذ موقع له على شبكة الإنترنت web-site أو إنشاء عنوان بريد إلكتروني E-mail لكي تنفتح أمامه آفاق جديدة من المعرفة والخدمات، ويصبح على اتصال بالعملاء في جميع أنحاء العالم، وبعملاء من مناطق جديدة كان يتعذر عليه الوصول إليهم من قبل إلا بصعوبة بالغة وعن طريق وسطاء وكثير من النفقات.

وفي المقابل انفتح المجال أيضًا أمام المستهلك للتعامل في الأسواق المحلية والعالمية بضغطة واحدة على لوحة مفاتيح جهاز الكمبيوتر لطلب المنتج أو الخدمة المعروضة، ودون حاجة إلى الدخول في علاقة مباشرة مع البائع، الأمر الذي أصبح يميز التجارة الإلكترونية عن التجارة التقليدية، حيث يظل البائع والمشتري على اتصال دائم بينهما في مجلس عقد حكمي

افتراضي رغم تباعد المكان والموقع بينهما.

على أنه يجب أن نضع في الاعتبار أنه ليس من السهل التوصل إلى تحديد واضح لمفهوم التجارة الإلكترونية، وذلك بالنظر إلى التطور السريع الحادث في تقنيات المعلومات والاتصالات، بالإضافة إلى اتساع دائرة الأنشطة التي تستخدم هذه التقنيات في إنجاز تلك المهام، وهو ما استلزم ضرورة التدخل لحماية هذه الأنشطة، كما تلزم حماية التاجر والموقع المنشأ على الشبكة الدولية للمعلومات بهدف الإعلان عن السلع والخدمات التي يسوِّقها.

وتعرض في هذه المواقع البيانات والمعطيات الخاصة بالمنتج أو موزع السلعة أو الخدمة مع تحديد مواصفات السلعة والخدمة، ووسائله وطرقه التي يستخدمها في تسليم السلع أو الخدمات التي يتم التعاقد عليها، وتتضمن هذه المواقع كذلك استمارات تطلب ذكر بيانات عن العميل نفسه، اسمه وعنوانه ورقم بطاقته الائتمانية، ووفقًا لذلك فقد تزايدت وسائل الحماية للتجارة الإلكترونية أشخاصها ومواقعها[1].

وسوف نقسم هذا الباب إلى ثلاثة فصول نبدأها بأساسيات التجارة الإلكترونية في فصل أول، ثم الحماية القانونية للتجارة الإلكترونية في فصل ثان، وفي النهاية تجارب التنظيم القانوني للتجارة الإلكترونية في فصل ثالث.

الفصل الأول: أساسيات التجارة الإلكترونية

الفصل الثاني: الحماية القانونية للتجارة الإلكترونية

الفصل الثالث: تجارب التنظيم القانوني للتجارة الإلكترونية

(1) د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007، ص 12.

الفصل الأول

أساسيات التجارة الإلكترونية

تمهيد وتقسيم:

تباينت الآراء الفقهية وتقارير المنظمات الدولية حول أساس التجارة الإلكترونية ومراحل تطورها، نظرًا لظهور العديد من المصطلحات التجارية حولها والتي تحتاج إلى المزيد من الإيضاح لتسهيل التعامل مع مكونات هذا المصطلح والظروف التي نشأت فيها هذه التجارة، ويرجع هذا التباين كذلك إلى التطور المستمر الذي يطرأ عليها، والتوسع في وسائلها وأساليبها، وبالتالي التوسع في مفهومها لارتباطها بشبكة الإنترنت التي تطورت بسرعة كبيرة، حتى إنه يتعذر على القواعد التنظيمية التي تضعها الدول اللحاق بها، ويرجع كذلك إلى اتساع السوق الناشئة، وهو ما انعكس على أساليب هذه التجارة وأوجد طرق اتصال وتسويق أكثر سهولة، مما أوجد الحاجة إلى ضرورة تنظيمها تنظيمًا قانونيًا، خصوصًا من حيث كيفية التعاقد، وحفظ حقوق المتعاقدين وإثباتها، وتقرير الحماية المدنية والجنائية لها ولأطرافها المتعاملين بها[1].

وقد مر استخدام شبكة الإنترنت في التجارة الإلكترونية بعدة مراحل ارتبط كل منها بالتطور المتلاحق الذي طرأ على استخدام الشبكة، ويمكن إجمالها في ثلاث مراحل هي:

---

(1) د. عبد الفتاح بيومي حجازي، حماية المستهلك في عقود التجارة الإلكترونية، بحث مقدم إلى مؤتمر حماية المستهلك المنعقد لدى الأمانة العامة لدول مجلس التعاون الخليجي بالرياض مع غرفة التجارة والصناعة بالرياض، في الفترة 18، 19 سبتمبر 2004، منشور في كتاب "مقدمة في الملكية الفكرية وحماية المستهلك"، دار الفكر الجامعي، الإسكندرية، 2005، ص 125.

المرحلة الأولى: حيث كانت المنشآت التجارية تستخدم شبكة الإنترنت في البداية كمجرد مواقع إعلانية تعرف العملاء ومتصفحي صفحات الويب web بنشاط المنشأة ومنتجاتها.

المرحلة الثانية: وهي أكثر تقدمًا، ونتيجة تزايد عدد مستخدمي شبكة الإنترنت، أدركت المنشآت التجارية أهمية التواجد الفعّال على الشبكة، فقامت بنشر المعلومات عن أنشطتها التجارية، كما امتلأت المواقع بالصور والرسومات الجذابة لمنتجات المنتجين وخدماتهم.

المرحلة الثالثة: في هذه المرحلة ونتيجة استخدام أحدث أنواع البرامج والتقنيات أصبح من السهل على العميل التعرف على مواقع شبكة الإنترنت التجارية من خلال عناصر التصفح البسيطة، والقيام بعمليات البيع والشراء بسهولة ويسر، وانتشرت تجارة الخدمات على مستوى واسع.

وسنتناول هذا الفصل من خلال مبحثين:

المبحث الأول: ماهية التجارة الالكترونية

المبحث الثاني: خصائص التجارة الإلكترونية ومعوقاتها ومستقبلها



المبحث الأول

ماهية التجارة الالكترونية

لقد كان للثورة المعلوماتية أثرها البالغ على تغيير محل التجارة الدولية، إذ مع التطورات التكنولوجية الناتجة عن ثورة المعلومات نجد أن التجارة الدولية لم تعد تنصب على المنتجات المادية، بل إن المنتجات الذهنية أصبحت تحتل مكانة بارزة في هذه التجارة كبرامج الكمبيوتر، وبنوك المعلومات، والدوائر الصناعية.

ولم يكن للثورة التكنولوجية أثرها على تغيير محل التجارة الإلكترونية فقط، بل أيضًا على وسائل إنجاز هذه التجارة، فعقود التجارة الدولية لم تعد تعتمد على الدعائم الورقية، فقد أحدثت المعلوماتية انقلابًا جذريًا في المفاهيم التقليدية للوثيقة المكتوبة، إذ حولتها من وثيقة ورقية إلى وثيقة إلكترونية.

ومن هنا كان الاهتمام الدولي بحماية حقوق الملكية الفكرية عبر شبكة الإنترنت، سواء من جانب منظمة التجارة العالمية (WTO) (World Trade Organization) أو من خلال المنظمة العالمية للملكية الفكرية (WIPO) World Intellectual Property Organization عن طريق متابعة تطبيق اتفاقية تريبس، التي خصصت بابًا مستقلا لحماية المنتجات الفكرية وخصوصًا منتجات المعلوماتية.

ومن ناحية أخرى فقد تعددت تعريفات التجارة الإلكترونية لحداثتها وتشعبها، مما دعا لجنة الأمم المتحدة للقانون التجاري الدولي إلى وضع قانون موحد للتجارة الإلكترونية في 1996/12/17، وهو يعد النموذج الذي تحتذي به كل الدول خلال وضع تشريعاتها المنظمة لقطاع التجارة الإلكترونية، وبالفعل سنت بعض الدول تشريعات تنظم التجارة

الإلكترونية[1]، مستلهمة مبادئ هذا القانون، وسوف نقسم هذا المبحث إلى أربعة مطالب وفق الترتيب التالي:

المطلب الأول: نشأة التجارة الإلكترونية

المطلب الثاني: تعريف التجارة الإلكترونية

المطلب الثالث: أشكال التجارة الإلكترونية

المطلب الرابع: تقدير التجارة الإلكترونية

(1) ومن أمثلة الدول التي صدر عنها تشريعات إلى الآن أستراليا عام 1999 " ELECTRONIC TRANSACTIONS BILL 1999 "، كولومبيا 1999، فرنسا قانون رقم 2000/230 بشأن تطويع قانون الإثبات لتكنولوجيا المعلومات والتوقيع الإلكتروني، هونج كونج مرسوم المعاملات التجارية الإلكترونية 2000، أيرلندا قانون التجارة الإلكترونية لسنة 2000، سنغافورة قانون التجارة الإلكترونية لسنة 1998، كوريا الجنوبية القانون الأساسي بشأن التجارة الإلكترونية لسنة 1999، الولايات المتحدة الأمريكية القانون الموحد للمعاملات الإلكترونية لعام 1999، وقد اعتمد من بعض الولايات (كاليفورنيا، بنسلفانيا، أوهايو، إنديانا، كنتاكي، مينسوتا، فرجينيا، جنوب داكونا، يزاسكا)، القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية قانون رقم 83 لسنة 2000, الأردن قانون المعاملات الإلكترونية رقم 2001/85، قانون إمارة دبي الخاص بالمعاملات والتجارة الإلكترونية قانون رقم (2) لسنة 2002، قانون مملكة البحرين بشأن التجارة الإلكترونية الصادر في 14 سبتمبر 2002، وقانون المعاملات والتجارة الإلكترونية رقم 1 لسنة 2006 لدولة الإمارات العربية المتحدة, وهناك مشروعات قوانين في مجموعة من الدول ومنها: مصر، الكويت، لبنان، تشيلي، بيرو، تايلاند، الهند، البرازيل، المملكة المتحدة.

المطلب الأول

نشأة التجارة الإلكترونية

ارتبط نشأة التجارة الإلكترونية بالتطور التقني الذي أدى إلى وجود شبكة الإنترنت، فأصبحت واقعًا تعيشه العديد من دول العالم وتبلغ التعاملات فيها بلايين الدولارات، وكما سبق توضيحه فقد كان التطور المعلوماتي هو الأساس الذي أوجد شبكة الإنترنت ومن ثم التجارة الإلكترونية، وسوف نتناول هذا المطلب من خلال ثلاثة فروع، الفرع الأول التطور المعلوماتي الإلكتروني، الفرع الثاني نشأة التجارة الإلكترونية وجذورها، والفرع الثالث أسباب نمو التجارة الإلكترونية وانتشارها وذلك على النحو التالي.

الفرع الأول

التطور المعلوماتي

تميزت كل مرحلة من مراحل التاريخ الإنساني بنوع معين من التكنولوجيا[1] تكنولوجيا الصيد، والزراعة، والصناعة، وأخيرًا تكنولوجيا الاتصالات والمعلومات، والتي أدت إلى تنامي دور المعلومات والمعرفة، وبزوغ ثورة تكنولوجيا المعلومات والتي أسهمت وبدرجة كبيرة في ظهور الكثير من المفاهيم الجديدة في كافة مناحي الحياة، وأفرزت مستويات غير مسبوقة من حيوية التأثير المتبادل بين أطراف المنظومات المعلوماتية،

(1) تكنولوجيا هي كلمة يونانية الأصل مشتقة من مقطعين الأول Techno بمعنى حرفة، والمقطع الثاني Logy بمعنى فن أو علم، أو Logic بمعنى منطق، ويقصد بلفظ Technologic في ترجمتها العربية علم الفنون أو الحرف أو علم الصناعة.

www.aflajgedu.gov.sa/vb/showthread.php?t=9341

وبات التنافس رهيبًا بين روافد العقل من المعلومات والمعارف، ونواتجه من الاختراعات والإبداعات[1].

كما شهد العالم في النصف الأخير من القرن العشرين مرحلة تحول أساسية، ليس في شكل النظام الدولي وتوازن القوى فحسب، بل من الناحية العلمية والإلكترونية أيضًا[2]،ومنها ارتياد الفضاء، واستنساخ الخلايا الحية[3]، وظهور الحاسب الآلي وتطوره، والذي يعود إلى عام 1964، عندما طور الباحثون الأمريكيون في جامعة بنسلفانيا أول جهاز يمكن اعتباره أداة إلكترونية كاملة البرمجة[4].

وإذا كانت بداية الثورة الصناعية قبل نحو مائتي عام قد أحدثت تغيرات في المجتمعات الإنسانية - إذ هجر الناس القرى إلى المدن، والمزارع إلى المجتمعات الصناعية- فإن الحاسب الإلكتروني (الكمبيوتر) قد غير من أنماط الحياة، وبدل من طبيعة الوظائف، وساهم في انفتاح المجتمعات الإنسانية[5]، حتى قيل بحق: إننا على أعتاب حضارة جديدة تمامًا[6] بما

---

(1) د. سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، 2006، ص 14.

(2) د. محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، النسر الذهبي للطباعة، بدون سنة طبع، ص3.

(3) د. محمد المرسي زهرة، حجية التوقيع الإلكتروني في الإثبات، بدون ناشر، وبدون سنة طبع، ص1.

(4) د. أسامة الخولي، الحاسوب هذا الطفل الذي ولد كبيرًا، مرجع سابق، ص 3، وكان ذلك على يد بعض العلماء وهم: Ch. Neumam، J. W. Maxuchly،J.P. E Chart استنادًا إلى أفكار عالم ألماني مشهور يسمي:(Van Nennam) .

(5) د. محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، مرجع سابق، ص3.

(6) د. أسامة الخولي، الحاسوب هذا الطفل الذي ولد كبيرًا، مرجع سابق، ص3.

أطلقه الحاسوب من ثورة معلوماتية، صاحبها ظهور أشكال جديدة للاتصال والتعامل من خلال شبكة الاتصالات الدولية، التي يطلق عليها اختصارًا إنترنت Internet، ويطلق عليها شبكة لأنها عبارة عن خطوط اتصال متشابكة، تربط أجهزة الكمبيوتر بعضها ببعض باستخدام خطوط التليفون[1]، وبدأت هذه الشبكة في ستينيات القرن الماضي، كما رأينا في الفصل التمهيدي، لخدمة عمليات التأهب السريع للقوات المسلحة الأمريكية، ثم انفصلت الشبكة العسكرية عن الشبكة الأم عام 1983، حينها سمح لمختلف الأفراد باستخدامها بعد سنوات قلائل، مما أدى إلى نشأة خدمة ويبWorld Web Wide ويرمز لها بـ WWW[2].

وكانت الحاسبات الإلكترونية[3] قد ظهرت مع بداية الستينيات، ثم أخذت في الانتشار إلى أن أمكن الأفراد العاديين اقتناؤها فضلا عن المؤسسات والشركات والمشروعات الفردية، واتخذت أشكالا عديدة؛ فمن حاسبات مكتبية، إلى حاسبات إلكترونية شخصية متنقلة يسهل على الأفراد حملها في أي مكان دون أدنى عناء، إلى حاسبات شخصية في الهواتف النقالة.[4]

(1) د. محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، مرجع سابق، ص4.
(2) د. إبراهيم أحمد إبراهيم، التجارة الإلكترونية والملكية الفكرية، مرجع سابق، ص590.
(3) للحاسبات الآلية مسميات عديدة في اللغة العربية بعد التعريب، مثل الحاسب الآلي، والحاسوب، أما في اللغة الإنجليزية فيسمي Computer اشتقاقا من الفعل Compute بمعني " يحسب "، وبالفرنسية Ordinateur.
(4) ومن المخترعات ساعة تمكن من تصفح شبكة الإنترنت، ويمكن وصلها بمجموعة غنية من المعلومات، ويعتبر استخدام الساعة الوسيلة المثلى للارتباط بالإنترنت باستمرار لانتشارها الواسع.
=

وهذا الانتشار الهائل للحواسيب بأشكالها المختلفة المتصلة بشبكة الإنترنت أوجد طوفانًا جارفًا من المعلومات غيَّر الحياة كلها كثيرًا سواء في ميادين العمل، أو في مجالات إبرام العقود، أو في مجال التعليم، ولعل أبرز أوجه التغير تتمثل في إلغاء المسافات، فالحواسيب تشترك كلها في منظومة واحدة للاتصالات، تغير الأفكار التقليدية في مجال التعاملات، كالتعاملات البنكية التي ابتدعت أشكالا جديدة بفضل المعلوماتية كالوفاء الإلكتروني وبطاقات الائتمان، وبطاقات السحب الآلي وغيرها، وكان للتجارة نصيب إذ ظهرت التجارة الإلكترونية " Electronic Commerce E. com أو Electronic Business " E.B في نهاية القرن العشرين.

وبظهورها أدت التجارة الإلكترونية إلى إبرام صفقات بين أشخاص بعيدين عن بعضهم البعض، وقد يكون أحدهم لم يسبق له أن التقى بالآخر، وهذا بالطبع يستلزم ضرورة توفير وسائل وأدوات لإتمام هذه الصفقات، وحماية مواقعها وأشخاصها.

الفرع الثاني

نشأة التجارة الإلكترونية وجذورها

انحصر الاهتمام في القرن التاسع عشر في كيفية تنمية مصادر الطاقة بشكل رئيسي، وقد صاحب ذلك قيام ثورة صناعية في منتصف هذا القرن، أدت إلى تغيرات شاملة في جميع مناحي الحياة، ومنها الجانب القانوني، حيث تم تطويع نظرياته وأحكامه لتتلاءم مع الجوانب والمشكلات الجديدة التي خلفتها تلك الثورة.

= مجلة "P.C. Magazine"، الطبعة العربية، السنة السادسة، العدد الثاني، مارس 2007، ص18.

أما في القرن العشرين وبالأخص في نصفه الثاني فقد ظهرت ثورة المعلومات وما صاحبها من تقنية خاصة لمعالجتها، وكان الكمبيوتر هو ركيزة هذه الثورة الهائلة[1].

ويرى البعض أن التجارة الإلكترونية ليست جديدة، بل إن جذورها ترجع إلى منتصف الأربعينيات عندما تم بناء أول كمبيوتر على أساس من المبادئ العامة للآلة التحليلية للمعلومات، والتي قام بوضعها تشارلز باباج مدرس الرياضيات بجامعة كامبردج عام 1830[2]، والذي توصل إلى إمكانية معالجة المعلومات بواسطة الآلة بشرط تحويلها إلى أرقام، والواقع أنه من الصعب تحديد الآباء الحقيقيين للكمبيوتر، إذ إن القسم الأكبر من الجهد الفكري والعملي بذله العلماء في الولايات المتحدة وبريطانيا خلال سنوات الحرب العالمية الثانية في ظل جو السرية المميز لوقت الحرب[3].

وفي أواخر الخمسينيات سخرت الشركات الكبرى الحاسبات لإيجاد نوع من التعامل الآلي بينها وبين الموردين الرئيسيين لها، وذلك عن طريق تركيب نهايات طرفية للحاسب الرئيسي للشركة الكبيرة عند الموردين

(1) محمد علي العريان، الجرائم المعلوماتية، مرجع سابق، ص 12.

(2) تشارلز باباج سبق الحديث عنه في الفصل التمهيدي، حيث ذكرنا أنه صمم أول حاسبة، وأسماها مكنة الفروق (difference engine)، ويعتبر بمثابة مخترع الحاسوب الميكانيكي.

(3) بيل جيتس، المعلوماتية بعد شبكة الإنترنت (طريق المستقبل) ترجمة عبد السلام رضوان، سلسة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، مارس 1998، ص 39.
والذي أشار إلى ثلاثة من المساهمين الرئيسيين هم كل من آلان تورنج، وكلود شانون، وجون فون نويمان.
والكتاب متوفر على العنوان التالي: http://www.maddawi.net/book

الأساسيين، بحيث يتاح للمورد الاطلاع على مستوى المخزون المتوفر لدى الشركة من الأصناف التي يقوم بتوريدها لها، ثم يقوم بناء على ذلك بتلبية متطلبات الشركة من هذه المواد وتغذية الحاسب بالبيانات مباشرة، وسميت هذه المرحلة بالارتباط بين الشركات الكبيرة والموردين الرئيسيين لها[1].

وفي منتصف الستينيات، بدأت مرحلة جديدة سميت بالتبادل الإلكتروني للبيانات(EDI) Electronic Data Interchange وذلك باستخدام الشبكات الخاصة، والتي انتشرت في السبعينيات لتسهيل الاتصال بين الأطراف، واختزال العمليات الورقية والتعامل البشري.

ويعتمد EDI بصورته التقليدية على شبكة تسمى شبكة القيمة المضافة VAN- Value -Added Network- فتقوم EDI بتجميع المعلومات والبيانات مثل بيانات المبيعات من عدة فروع وطلبات شراء للموردين، وترسل EDI هذه المعلومات إلى VAN حيث يوجد به صندوق بريد إلكتروني يسمح بالاتصال المباشر بأجهزة حواسب الشركاء، وأدى هذا إلى سرعة إرسال البيانات وزيادة كفاءة العمليات، وساعد على تخفيض التكاليف التشغيلية، وإتاحة فرص الوصول إلى أسواق أكثر اتساعًا، بالإضافة إلى صلاحية تطبيق هذه التقنية في مختلف أنواع الأعمال.[2]

وفي الوقت الذي استخدمت فيه جميع أنواع الأعمال EDI لتقديم الطلبات وإرسال الفواتير بدأ تجار التجزئة استخدام الإعلان التلفزيوني لتوريد طلبات عبر التليفون من الجمهور العام بالنسبة لكل أنواع البضائع، كما كانت البنوك أيضًا تستخدم EFT وهو تحويل الأموال إلكترونيًا لنقل

(1) رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص126.
(2) د. سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، بحوث ودراسات شرطية، شرطة دبي، العدد91، 1999.

الأموال حول العالم.[1]

والحديث عن التجارة الإلكترونية لا ينفصل عن الشبكة الدولية، فشبكة الإنترنت كما, سبق وأن عرفناها, هي (شبكة كمبيوتر عملاقة) وأنها أكبر شبكات الكمبيوتر على سطح هذا الكوكب، واسم (إنترنت Internet) مشتق من اللغة الإنجليزية (Interconnection Network)، أي شبكة التشبيك بمعنى أنها شبكة تربط مجموعة من أجهزة الكمبيوتر المتصلة ببعضها البعض وتستطيع تبادل المعلومات فيما بينها[2]، باعتبارها الوسيلة الأساسية للاتصالات.

وقد عرف الإنسان التبادل منذ بداية الخليقة، وكانت العقود بين طرفين في مكانين مختلفين تتم من خلال الرسول الذي يتكفل بنقل إرادة كل منهما إلى الآخر من أجل إتمام عملية التعاقد، وبعد اختراع وسائل الاتصال عن بُعد مثل التليفون والتلغراف والتلكس بدأ الإنسان يتخذ خطوات واسعة نحو المعاملات الإلكترونية، واتسعت الأمور مع ظهور الكمبيوتر في مجال الاتصالات وظهور ما يسمى بالتعاقد عن بعد.

وقد بدأ التحول الجذري في مجال المعاملات بالتبادل الإلكتروني بالبيانات منذ بداية السبعينيات من القرن الماضي، حيث كانت التجارة

(1) د. طارق عبد العال، التجارة الإلكترونية، الدار الجامعية، 2005، ص 22.

(2) كما اعتبر البعض أن كلمة (إنترنت) إنجليزية الأصل، واعتبروها أنها اختصار مزجي للحروف الأولى من كلمتي (International) بمعنى دولي، و(Net Work) بمعنى شبكة، وظهر أول ربط بين الحاسب وأجهزة الاتصال في عام 1940، إلى أن أصبحت الحاسبات الشخصية (PCS) تستطيع الارتباط بشبكات الاتصال والاستفادة من المعلومات المخزنة والمتبادلة عبر خطوط الاتصال. في المعنى ذاته: د. عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود، رسالة دكتوراه، جامعة القاهرة، 1998، ص 31.

الإلكترونية تعتمد نظامًا واسعًا من التكنولوجيا لتبادل المعلومات لتسهيل عملية التعاقد بين أطراف المبادلة التجارية واختزال العمليات الورقية، واعتبر ذلك أوفر في التكاليف وأسرع في تلبية حاجات التجارة والتسليم في الميعاد، خصوصًا إذا كان يتم بطرق سليمة وآمنة وقانونية[1].

وكان التبادل وفقا لهذا النظام يتم بين أصحاب المعاملات التجارية من خلال اتفاقيات تبادل، وهو نظام ليس في وسعه تلبية حاجات المعاملات والمبادلات الإلكترونية التي تتم بين أطراف لا يعرف أحدهما الآخر ولا توجد بينهم شراكة تجارية.

واتبعت العديد من الشركات والمؤسسات فيما بعد تقنية أخرى في مجال التجارة الإلكترونية عن طريق إرسال رسائل عبر البريد الإلكتروني وشبكة الإنترنت، والعمليات التي تتم عبر الشبكة العنكبوتية، وقد أصبغت الدراسات الاقتصادية والاجتماعية والقانونية وصف عصر المعلومات على الحقبة الزمنية الممتدة من سبعينيات القرن العشرين حتى الآن، فيما يتجه البعض الآخر إلى أن ذلك يبدأ من مطلع الثمانينيات[2].

وتزايدت أعداد المتعاملين مع هذه الشبكة وخصوصًا بعد السماح للأفراد العاديين باستعمالها[3]، وحقق استخدامها معدلات نمو مذهلة، فعدد مستخدميها يتضاعف سنويا، وأقبل رجال الأعمال وأصحاب المؤسسات على استخدام الشبكة في الأغراض التجارية، وأصبحت عمليات الاتصال

(1) د. محمد حسام لطفي، الإطار القانوني للمعاملات الإلكترونية، مطبعة النسر الذهبي، القاهرة، 2002، ص 9.

(2) د. سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، مرجع سابق، ص1.

(3) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، مرجع سابق، ص4.

بين البائع والمشتري وعمليات المفاوضة والمعاينة حول السلع تتم بسرعة وسهولة، وكذلك عمليات إتمام الصفقات التجارية بين الشركات.

وقد أدى ذلك الأمر إلى اهتمام الدول بضرورة وجود بيئة تشريعية محكمة وشاملة تستطيع استيعاب جميع تعاملات التجارة الإلكترونية التي تتحرك بمعدل سريع لكي تضمن بقاءها في إطار قانوني سليم وملائم، ونتيجة لما حصل من تطور في الأوضاع العالمية الراهنة وما تبع ذلك من تغيرات في السوق العالمي فرض على جميع الدول الامتثال لها دون وجود هامش للاختيار، مما جعلها جميعًا مطالبة بتوفير البيئة القانونية المناسبة للتجارة الإلكترونية، وإلا فإنها ستكون على هامش الاقتصاد العالمي الجديد أو ما يعرف بالاقتصاد الرقمي[1].

(1) تستحوذ الدول المتقدمة التي يقطنها نحو 15% من سكان العالم على حوالي 88% من مستخدمي شبكة الإنترنت، بينما تبلغ نسبة المشتركين في شبكة الإنترنت في دول جنوب آسيا التي يقطنها نحو 20% من سكان العالم ما نسبته 1% فقط، أما في إفريقيا التي يقطنها 12% من سكان العالم فإن عدد المشتركين يبلغ نحو مليون شخص، وتمتلك 14 مليون خط هاتف "أي أقل من عدد الخطوط في مدينة طوكيو وحدها أو في حي مانهاتن في مدينة نيويورك" وتتركز 80% منها في 6 دول فقط في القارة الإفريقية.
ويقدر عدد مستخدمي شبكة الإنترنت بنحو 294 مليون شخص في نهاية 2001 في الولايات المتحدة الأمريكية، مقابل 123 مليونًا في أوروبا الغربية، و836 مليونًا في دول آسيا المطلة على الهادي بما فيها اليابان، و411 مليونًا في باقي دول العالم.
فيما أوردت دراسة أخرى إحصائيات عن وضع اقتصاد تكنولوجيا المعلومات والتجارة الإلكترونية في العالم عمومًا والمنطقة العربية على وجه التحديد، والتي قدرت عدد مستخدمي شبكة الإنترنت في عام 2001 بنحو 200 مليون شخص بعدما كان نحو 100 مليون عام 1998، وقدرت هذه الإحصائيات عدد المشتركين في شبكة الإنترنت بحوالي 2% من سكان العالم فقط رغم أن أعدادهم تتضاعف=

من ناحية أخرى يزداد عدد الشبكات التي تتكون منها شبكة الإنترنت بشكل مطرد[1]، وكلما زاد عدد الشبكات وعدد أجهزة الكمبيوتر الخادمة زاد بالتالي عدد المستخدمين المرتبطين بشبكة الإنترنت، وهناك إحصائية تقول أن هناك مليوني مستخدم ينضمون إلى شبكة الإنترنت كل شهر، أي بمعدل 46 مستخدمًا جديدًا كل دقيقة، ويوجد أعلى عدد للمستخدمين في العالم في الولايات المتحدة الأمريكية، ويتوقع أن يكون العدد في الصين والهند[2] أكبر

= بسرعة غير مسبوقة.

وبلغ عدد مواقع شبكة الإنترنت العاملة في الدول المتقدمة 312 موقعًا لكل 1000 إنسان في يوليو 1999م، مقابل 6 مواقع فقط لكل 1000 إنسان في الدول النامية، علمًا بأن عدد المواقع الإجمالية في العالم في الفترة نفسها بلغ 256 مليونًا.

ويوجد في كندا والولايات المتحدة نحو 36,5% من إجمالي عدد مواقع شبكة الإنترنت البالغ عددها 256 مليونًا في يوليو 1999م، مقابل 42,2% في أوروبا، و46% في أستراليا واليابان ونيوزيلندا، وبلغ معدل النمو في مواقع شبكة الإنترنت في العام 1999م نحو 18% في إفريقيا، و74% في أمريكا الشمالية، و36% في أمريكا اللاتينية، و61% في آسيا، و30% في أوروبا.

وبلغ عدد الحواسيب المضيفة للإنترنت في جميع أنحاء العالم 5846 ألفًا في يناير 1995، وارتفع بشكل تدريجي حتى وصل إلى 36739 ألفًا في يوليو 1998م.

ويقدر عدد الأشخاص لكل وحدة من وحدات خدمة شبكة الإنترنت بحوالي 50 وحدة في الولايات المتحدة، 70 في كندا، 60 في أستراليا، 90 في هولندا، 125 في سنغافورة، 130 في المملكة المتحدة، 180 في ألمانيا، 310 في هونج كونج، 470 في اليابان، 930 في جنوب إفريقيا، 87000 في إندونيسيا، 561000 في الصين، 1200000 في الهند.

http://www.thegulfbiz.com/archive/index.php/t،1544.html

(1) مصطفى السيد، دليلك إلى شبكة الإنترنت، مرجع سابق، ص 15.

(2) أصبحت مدينة بنغالور في الهند مركزًا نشطًا من مراكز الابتكار، حيث يوجد بها ما يزيد على 300 شركة من شركات التكنولوجيا الرفيعة، وتقدر صادرات الهند من=

من الولايات المتحدة الأمريكية حسب تقرير هيئة صناعة الكمبيوتر (www.c-i-a.com)، وذلك لعامل التعداد السكاني والاستثمارات الضخمة في البنية التحتية[1].

وعمومًا فإن التجارة الإلكترونية والعلاقات الناشئة عنها تثير العديد من التحديات القانونية، تتمثل في التعاقد الإلكتروني، صحة البيانات، وسائل الإثبات، حجية الدليل الرقمي[2]، الرسائل الإلكترونية، الدفع الإلكتروني، الملكية الفكرية، الاختصاص القضائي، الحماية المدنية والتقنية والاقتصادية والجنائية لأطراف التجارة.

ولا يسعنا في النهاية إلا أن نشير إلى أن الوطن العربي وبالرغم من الثورة الإلكترونية التي تجتاح العالم فإنه ما زال متأخرًا فيها، وإن شهدت بعض الدول العربية تطورًا ملحوظًا في هذا الجانب في محاولة منها للحاق بركب التقدم العلمي, والتشريعي وكان الأسبق فيها المشرع التونسي الذي أصدر القانون رقم 2000/83 الخاص بالمبادلات والتجارة الإلكترونية.

= البرمجيات بـ4 بلايين دولار في عام 2003، أي قرابة 9 في المائة من مجموع صادرات الهند.
ttp://www.alarabiya.net/views/2005/06/25/14298.html

(1) في عام 1998 كان عدد الموصولين بشبكة الإنترنت 143 مليون شخص فقط، ولكن في عام 2001 ارتفع هذا العدد إلى 700 مليون شخص، وفي عام 1996 بلغت معاملات سوق التجارة الإلكترونية 2.6 بليون دولار، وفي عام 2002 ارتفعت إلى 300 بليون دولار، وأصبح للإنترنت بالفعل نطاق من التطبيقات يفوق في اتساعه أي وسيلة أخرى سبق اختراعها من وسائل الاتصال. مشار إليه في: د. عمر محمد أبو بكر بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مرجع سابق، ص 72.

(2) د. هلالي عبد اللـه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2006، ص 25.

تبعه قانون المعاملات الإلكترونية الأردني رقم 85 /2001، ثم قانون إمارة دبي رقم 2002/2 بشأن المعاملات والتجارة الإلكترونية، والقانون الاتحادي الإماراتي رقم 2006/1 بشأن المعاملات والتجارة الإلكترونية والقانون رقم 2006/2 في شأن مكافحة جرائم تقنية المعلومات.[1]

---

(1)http://www.midle.eastonline.com، http://www.computerconomics.com

تُظهر الأرقام عن الواقع الحالي لاقتصاد تكنولوجيا المعلومات والتجارة الإلكترونية في العالم العربي بشكل واضح الحجم الكبير للفجوة الرقمية في المنطقة العربية مقارنة مع مناطق العالم الأخرى؛ حيث يقدر عدد مشتركي شبكة الإنترنت في الدول العربية في عام 2000 بنحو 550 ألف مشترك، منهم 29% في دولة الإمارات، و18% في السعودية، و12% في لبنان، و10% في مصر، ويقدر عدد مستخدمي شبكة الإنترنت في الدول العربية بنحو 19 مليون شخص بمعدل 35 مستخدمًا لكل اشتراك، إلا أن تقديرات أخرى صدرت خلال الربع الأول من العام 2002 تبدو متفائلة بشكل أكبر حيث تضاعف الرقم، لكنه يبقى رقمًا متواضعًا بسبب مشاكل الفقر والأمية والجهل والصحة... وتمثل نسبة مستخدمي شبكة الإنترنت في الدول العربية نحو 0.6% من عدد مستخدمي شبكة الإنترنت في العالم الذي بلغ 304 ملايين شخص و0.7% من إجمالي عدد السكان في الدول العربية الذي يبلغ حوالي 275 مليون نسمة.

وتتوزع استخدامات شبكة الإنترنت على 59% لإرسال البريد الإلكتروني، و22% لتصفح المعلومات، و13% لأغراض العمل، و6% لأغراض التجارة الإلكترونية، ويقدر حجم الإنفاق على المعلوماتية في الدول العربية بنحو 20 دولارًا للفرد، كما تقدر نسبة الإنفاق على البحث والتطوير للناتج المحلي الإجمالي للدول العربية نحو0.4% فقط، ويقدر وجود 40 جهاز هاتف نقال لكل 1000 شخص في الدول العربية عام 1999م..

http://www.thegulfbiz.com/archive/index.php/t،1544.html

وأشارت إحصائية حديثة قام بها موقع إحصائيات شبكة الإنترنت العالمية إلى أن آسيا تصدرت إجمالي مستخدمي شبكة الإنترنت حسب إحصائية ديسمبر 2007، =

= حيث بلغ إجمالي مستخدمي شبكة الإنترنت في قارة أسيا 459.476 مليون مستخدم، وجاءت أوروبا في الترتيب الثاني بإجمالي عدد مستخدمين بلغ تقريبًا337.878 مليون مستخدم، وتأتي أمريكا الشمالية في المرتبة الثالثة من حيث عدد المستخدمين 234.788 مليون مستخدم، ثم أمريكا اللاتينية والكاريبي 115.759 مليون مستخدم، وجاءت إفريقيا خامسًا بـ 43.700 مليون مستخدم.

ويلاحظ أن اللغة العربية هي أكثر اللغات تحسنًا في عدد المستخدمين، حيث تضاعف عدد المستخدمين بحوالي 10 أضعاف ما بين عامي 2000و2007م، حيث بلغ إجمالي المتحدثين باللغة العربية حسب إحصائية الموقع 350.965.119 مليون شخص، بينما بلغ مستخدمو شبكة الإنترنت منهم 46.359.140 مليون مستخدم.

الجدير بالذكر أن ما نسبته حوالي 60% من مستخدمي شبكة الإنترنت في العالم العربي موجودون في منطقة الخليج العربي، حيث تكون تكاليف شراء الكمبيوترات واشتراك شبكة الإنترنت أقلّ بكثير من الدول الأخرى، بالإضافة إلى كون الكثير من هذه الدول تواكب التقنية بشكل مستمر وتقوم بتطوير البنية التحتية للإنترنت، بينما تنخفض النسبة بشكل ملحوظ في الدول الإفريقيّة، مع وجود العراق كحالة خاصّة بسبب الأوضاع السياسيّة فيه.

وبالنسبة لأعلى 20 دولة التي يوجد فيها أكبر عدد من مستخدمي شبكة الإنترنت في العالم في عام 2007، فإنّ خطوات الدول العربيّة تبدو خجولة، حيث لم تصل أيّ منها إلى هذه اللائحة، وحصلت الولايات المتحدة الأميركيّة على المرتبة الأولى بعدد 211.1 مليون مستخدم (من أصل 302 مليون مواطن)، بينما كانت المرتبة 20 من نصيب الأرجنتين بعدد 13 مليون مستخدم (من أصل 38.2 مليون مواطن).

وبالنسبة لترتيب الدول العربية فقد شكل ارتقاء المغرب إلى المرتبة الأولى في العالم العربي من حيث عدد مستخدمي شبكة الإنترنت لسنة 2007 مفاجأة لكل المتتبعين بعد أن كان يحتل المرتبة السابعة قبل سبع سنوات، إذ بلغ عدد المغاربة المستعملين للشبكة المعلوماتية هذا العام 6.1 مليون، متقدمًا على مصر بـ6 مليون والسودان بـ3.5 مليون، ثم السعودية التي استقرت لسنين في 2,54 مليون، والجزائر بـ2.46 مليون ثم العراق في ذيل القائمة بـ32 ألف مستخدم.

واحتلت دولة الإمارات الصدارة من حيث نسبة المستخدمين من إجمالي السكان،=

الفرع الثالث

أسباب نمو التجارة الإلكترونية وانتشارها

شكّل ظهور (شبكة الإنترنت) وانتشارها الواسع مفاجأة للكثير من المحللين والمستخدمين، وأثير تساؤل حول أسباب الانتشار والنمو السريع لهذه الشبكة التي تعتبر من حيث العمر حديثة جدًا، والتي هي أداة التجارة الإلكترونية ووسيلتها في الانتشار، وترجع أسباب هذا النمو إلى عدة أسباب

= حيث بلغت النسبة 33.3%، تلتها دولة قطر بـ26.6% ثم الكويت بـ25.6% فالبحرين بـ21 % ثم المغرب بـ20.%، يذكر أن عدد المغاربة المستخدمين للإنترنت لم يتعد مائتي ألف سنة 2000، وكان يصنف في المركز السابع بعد الإمارات ومصر ولبنان بـ735 ألف و450 ألف و300 ألف على التوالي , وكانت الإمارات تحتل المرتبة الأولى عام 2000.
أمّا بالنسبة لعدد المستخدمين في كلّ دولة عربية (مارس 2007) فإنّ الأعداد هي: مصر 5.5 مليون، المغرب 4.6 مليون، السودان 2.8 مليون، المملكة العربية السعودية 2.54 مليون، الجزائر 1.92 مليون، الإمارات العربية المتحدة 1.397.200، سوريا 1.1 مليون، تونس 953 ألفا، الكويت 700 ألف، الأردن 629.500 ألف، لبنان 600 ألف، اليمن 330 ألفا، عُمان 285 ألفا، فلسطين والبحرين 155 ألفا، الصومال 90 ألفا، العراق 36 ألفا، موريتانيا 20 ألفا، جيبوتي 10 آلاف.
أمّا نسبة السكان الذين يستخدمون شبكة الإنترنت بشتى أنواعها (العادية وعالية أي عريضة النطاق) لتعداد السكان في الدولة، فهي كالتالي: الإمارات العربية المتحدة 35.1%، قطر 26.6%، الكويت 25.6%، البحرين 24,3%, لبنان 15.4%، المغرب 15.1%، الأردن 11.7%، المملكة العربية السعودية 10.6%، عُمان 10%، تونس 9.2%، فلسطين 7.9%، السودان 7.6%، مصر 6.9%، الجزائر 5.7%، سوريا 5.6%، ليبيا 3.3%، جيبوتي 1.1%، اليمن 1%، الصومال 0.7%، موريتانيا 0.5%، العراق 0.1%.
.www.internetworldstats.com

نذكر منها ما يلي:

- الثورة في مجال الاتصالات التي شهدها العالم في الحقبة الأخيرة، والتحول الجذري في هذا المجال من الأسلوب العادي المتعارف عليه إلى أساليب أحدث في جميع وسائل الاتصالات المستخدمة في الحياة اليومية.
- تحول الاقتصاد إلى العالمية، مثل ترابط أسواق المال والبورصات العالمية، وانتشار المعاملات المالية على مستوى عالمي، وتأثرها بالزيادة أو النقصان بالأحداث الجارية في العالم.
- تنوع الخدمات الإعلامية والإعلانية والحاجة لبثها لجميع الشعوب وبطريقة سهلة وبتكلفة أقل.
- اعتماد عملية اتخاذ القرار في المؤسسات على المعلومات الخارجية أكثر من المعلومات الداخلية في شتى المجالات (الاقتصادية، والسياسية، والقانونية، والتعليمية، والسياحية، وغيرها من المجالات).
- الاتجاه المتزايد لمؤسسات الأعمال نحو تقليص العمالة والاستعاضة عنها بالأجهزة الحديثة والتقنيات، واكتساب المهارات عن بعد، والاستفادة من عمل الآلة وإنتاجيتها على حساب الفرد بهدف توفير التكلفة وتخفيض الوقت.
- الحاجة لربط الأنظمة ومواقع العمل بعضها ببعض من جهة، ومع الإدارة المركزية من جهة أخرى.
- التوسع في تقديم الخدمات إلى المنازل كخدمات البنوك والتسوق والسياحة بالإضافة إلى خدمة المعلومات.
- الاهتمام المتزايد بمعرفة المستجدات الحديثة على الساحة الدولية ومعرفة آخر الأخبار والتطورات بسرعة، الأمر الذي يتطلب وجود

بنوك للمعلومات ومراكز للبحوث.

- استفادة المناطق النائية والريفية من الخدمات التعليمية والإعلامية والثقافية والصحية والقانونية وغيرها[1].

يضاف إلى ما سبق أن شبكة الإنترنت ليست مؤسسة خاصة بفرد من الأفراد أو جهة معينة تملكها، بل هي شبكة عالمية واسعة تتصل بها مئات الآلاف من الشبكات الأخرى، لذلك فإن عملية الاتصال بها سهلة وغير مكلفة كثيرًا؛ لأنها لا تستلزم دفع مبالغ مادية إلى جهة مركزية واحدة في العالم، بل تتم العملية بشكل مشابه للاتصالات الهاتفية، حيث يقوم المستفيد بأداء المبالغ المستحقة لقاء اتصالاته إلى الجهة المشرفة على شبكته الإقليمية، أما الحصول على المعلومات أو الخدمات فهو شيء آخر قد يكون مجانيًا أو بعملية تجارية بسيطة يتم تسديد قيمتها إلى مقدم الخدمة، وذلك عن طريق الاشتراك، أو الشراء المباشر من الموقع، سواء باستخدام البطاقات الائتمانية أو التحويل النقدي أو شيك بقيمة المبلغ[2].

المطلب الثاني

تعريف التجارة الإلكترونية

شهدت السنوات القلائل الأخيرة تزايد حجم التجارة الإلكترونية بالنسبة إلى حجم التجارة الدولية، فلم تكن التقديرات المتعلقة بها تتجاوز ملايين الدولارات على المستوى العالمي، إلا أنه في سنوات قليلة تعاظمت هذه

(1) د. إبراهيم أحمد إبراهيم، التجارة الإلكترونية والملكية الفكرية، مرجع سابق، ص591.

(2) د.عصام فايد، مسئولية البنك عن فحص المستندات في الاعتماد المستندي، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 2007، ص 68.

التجارة، فأصبحت المعاملات الإلكترونية تقدر بالبلايين[1].

وقد لفت هذا التزايد المستمر في حجم المعاملات الإلكترونية انتباه الدول والمنظمات الدولية، وتم وضع أول إطار للتنظيم القانوني الدولي لمعاملات التجارة الإلكترونية في اتفاقيات منظمة التجارة العالمية الموقعة في مراكش بالمغرب في 15 أبريل سنة 1994[2]، وجرت محاولات عديدة لتعريفها ما بين تعريف فقهي، وتعريف للمنظمات الدولية والإقليمية وتعريف تشريعي.

وينبغي عدم الخلط بين مصطلح التجارة الإلكترونية Electronic- Commerce ومصطلح الأعمال الإلكترونية Electronic- Business، فهما ليسا مصطلحين مترادفين وإنما هما مصطلحان مختلفان، فالأعمال الإلكترونية أوسع مجالا وأكثر شمولية، فهي تشمل التجارة الإلكترونية والبنوك الإلكترونية والحكومة الإلكترونية وشركات التأمين الإلكترونية، في حين أن التجارة الإلكترونية نشاط تجاري ولا سيما التعاقدات حول طلب المنتجات والخدمات باستخدام وسائل إلكترونية وضمن بيئة إلكترونية.

---

(1) بلغت حصة السوق للعديد من الشركات في مجال التجارة الإلكترونية أرقامًا فلكية حيث وصلت في حالة (أمازون دوت كوم) 22 بليون دولار، وشركة (إيباي) 23 بليون دولار، وشركة (إي تويز) 1.7 بليون دولار، وشركة (بارنز آند نوبل) 1.1 بليون دولار أمريكي، كما بلغت في شركة (سيرز) 10.5 بلايين دولار، وفي شركة (سويشباير) 1.2 بليون دولار، وفي شركة (تويز آر يو إس) 2.8 بليون دولار، وشركة (بورز) 1.1 بليون دولار أمريكي. http://www.arabcin.net

د. إبراهيم أحمد إبراهيم، التجارة الإلكترونية والملكية الفكرية, مرجع سابق، ص592.

(2) المرجع السابق، ص 593.

ولقد تعددت تعريفات التجارة الإلكترونية وأصبح من الصعوبة الاتفاق على تعريف محدد، خصوصًا إذا أخذنا في الاعتبار طبيعة التقنية المستخدمة في هذه التجارة، والتي تعتمد على عناصر تميزها هي: النشاط التجاري، والدعائم الإلكترونية، والعولمة، وأيضًا نظرًا للتطور المستمر الذي يطرأ عليها مما يؤدي إلى تطوير وسائلها وأساليبها، وتوسيع أهدافها ومفهومها، ونظرًا لاختلاف مجالات تطبيقها، وقيام كل مجال بتفسيرها من وجهة النظر التي تخدمه، ولبيان ذلك نقسم هذا المطلب إلى فروع ثلاثة: الأول التعريف الفقهي للتجارة الإلكترونية، والثاني تعريف التجارة الإلكترونية في المنظمات والوثائق الدولية، والثالث التعريف في القوانين الوطنية.

الفرع الأول

تعريف الفقه للتجارة الإلكترونية

اختلف الفقه في وضع تعريف للتجارة الإلكترونية، فعرفها البعض بأنها عملية البيع والشراء عبر الشبكات الإلكترونية على المستويين السلعي والخدمي بجانب المعلومات وبرامج الكمبيوتر والأنشطة الأخرى التي تساعد على الممارسات التجارية، أو لتنفيذ بعض أو كل المعاملات التجارية في السلع والخدمات التي تتم بين مشروع تجاري وآخر، أو بين مشروع تجاري ومستهلك، باستخدام تكنولوجيا المعلومات والاتصالات[1].

كما عرفها آخرون بأنها العملية التجارية التي تتم بين طرفين ـ بائع ومشتر ـ وتتمثل في عقد الصفقات وتسويق المنتجات عن طريق استخدام

(1) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص39.

الحاسب الإلكتروني عبر شبكة الإنترنت، وذلك دون حاجة لانتقال الطرفين للقائهما، بل يتم التوقيع إلكترونيًا على العقد"[1]، أو أنها " كل معاملة تجارية تتم عن بُعد باستعمال وسيلة إلكترونية حتى إتمام العقد"[2]، أو أنها " أداء العملية التجارية بين شركاء تجاريين باستخدام تكنولوجيا معلومات متطورة بغرض رفع كفاءة وفاعلية الأداء ".

كما حاول جانب من الفقه المصري وضع تعريف للتجارة الإلكترونية فعرفها بأنها: "جميع المعاملات التي تتم عبر شبكة الإنترنت حتى لو لم تتمتع بالصفة التجارية". وأضاف أن التجارة الإلكترونية لا تختلف في مفهومها عن التجارة التقليدية بمفهومها كممارسة العمل التجاري على وجه الاعتياد، ولكن ترجع خصوصيتها إلى وسائل مباشرتها[3].

ويعود هذا الاختلاف إلى اختلاف نظرة الفقهاء إلى التجارة الإلكترونية، فمنهم من توسع في تعريف التجارة الإلكترونية، وذلك بأن أدخل فيها جميع الأعمال سواء أكانت تجارية أو غير تجارية[4] إذا ما تمت بطريقة إلكترونية

---

(1) د. فاروق حسين، البريد الإلكتروني، مرجع سابق، ص 9.

(2) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، 2004، ص 49.

(3) هند محمد حامد، التجارة الإلكترونية في المجال السياحي، رسالة ماجستير، كلية السياحة والفنادق، جامعة حلوان، ص 11.

(4) نصت المادة (4) من قانون المعاملات التجارية لدولة الإمارات العربية المتحدة رقم 18 لسنة 1993 على أن الأعمال التجارية هي:

(4) الأعمال التي يقوم بها التاجر لشئون تتعلق بتجارته، وكل عمل يقوم به التاجر يعتبر متعلقا بتجارته ما لم يثبت غير ذلك.

(4) أعمال المضاربة التي يقوم بها الشخص ولو كان غير تاجر بقصد تحقيق الربح.

(4) الأعمال التي ينص القانون على اعتبارها أعمالا تجارية.

(4) الأعمال المرتبطة أو المسهلة لعمل تجاري. =

أيًا كانت هذه الوسيلة، في حين ضيق البعض في تعريف التجارة الإلكترونية حتى حصرها في وسيلة معينة هي شبكة الإنترنت العالمية، كما ظهرت تعريفات مخصصة للتجارة الإلكترونية.

وسوف نستعرض التعريفات الفقهية بالتقسيم الآتي:

1) **التعريف الضيق للتجارة الإلكترونية**

2) **التعريف الموسع للتجارة الإلكترونية**

3) **التعريف المخصص للتجارة الإلكترونية**

ونستعرض كل قسم منها على النحو التالي:

1 - التعريف الضيق للتجارة الإلكترونية:

عرَّف أصحاب هذا الاتجاه التجارة الإلكترونية في نطاق ضيق، بحيث تشمل أنشطة البيع والشراء وتقديم الخدمات عبر شبكة الإنترنت، فالتجارة الإلكترونية عندهم هي (العملية التي تتم بين طرفين - بائع ومشتر أو أكثر - عن طريق استخدام الكمبيوتر عبر شبكة الإنترنت)[1].

ويحد هذا التعريف من نطاق التجارة الإلكترونية فيعتبرها بيعًا وشراءً عبر شبكة الإنترنت، وهذا ينافي واقع التجارة الإلكترونية التي بدأت تتجاوز ذلك إلى صور عديدة من الأعمال التجارية كالإعلان وإنشاء المواقع والمتاجر الافتراضية وإدارتها، وتقديم العديد من الخدمات كخدمة الاتصالات والتعاملات المصرفية.

كما ظهرت تعريفات مضيقة أخرى للتجارة الإلكترونية حاولت حصر

= كما نصت المادة (5) على الأعمال التي تعد تجارية بحكم ماهيتها، والمادة (6) بينت الأعمال التجارية التي تزاول على وجه الاحتراف.

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، 2000، ص 5.

هذه التجارة في مجموع الأنشطة التجارية المؤدية إلى إبرام تعاقدات عن بُعد، دون تطلب ضرورة الوفاء بقيمة هذه التعاقدات بالوسيلة نفسها، ويقترب من هذه التعريفات التعريف القائل بأن التجارة الإلكترونية هي تنفيذ بعض أو كل المعاملات التجارية في السلع والخدمات التي تتم بين مشروع تجاري وآخر، أو بين مشروع تجاري ومستهلك، وذلك باستخدام تكنولوجيا المعلومات.[1]

2- التعريف الموسع للتجارة الإلكترونية:

وضع أصحاب هذا الاتجاه تعريفًا موسعًا للتجارة الإلكترونية، بحيث يشمل كل نشاط مهما كانت طبيعته، فهي تتعلق بتبادل السلع أو الخدمات والتي تتم عبر شبكة الإنترنت أو باستخدام الوسائل الإلكترونية.

فالتجارة الإلكترونية عندهم هي: " التجارة التي تشتمل على أنواع ثلاثة مختلفة من الصفقات هي تقديم خدمات شبكة الإنترنت، والتسليم الإلكتروني للخدمات أي تسليم صفقات المنتجات الخدمية للمستهلك في شكل معلومات رقمية، واستخدام شبكة الإنترنت كقناة لتوزيع الخدمات، وعن طريقها يتم شراء السلع عبر الشبكة، ولكن يتم تسليمها بعد ذلك للمستهلك في شكل غير إلكتروني"[2].

---

(1) د. حسن الماحي، نظرات قانونية في التجارة الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، في الفترة من 26: 28 أبريل 2003، ص 180. انظر كذلك: د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص 36، والذي أشار إلى ورود هذا التعريف في التقرير الصادر عن لجنة التجارة الإلكترونية بمركز المعلومات ودعم اتخاذ القرار برئاسة مجلس الوزراء بجمهورية مصر العربية بعنوان "مقترح المبادرة المصرية للتجارة الإلكترونية 1999".

(2) د. إبراهيم أحمد، تقرير عن الجوانب القانونية للتجارة الإلكترونية في مصر، =

وعرفت بأنها: " جميع المعاملات التي تتم عبر شبكة الإنترنت حتى ولو لم تتمتع بالصفة التجارية، وإن كان الغالب أن تتمتع بهذه الصفة من جانب مقدم السلعة أو الخدمة على الأقل، والذي غالبًا ما يكون تاجرًا".[1]

وانتقد هذا الاتجاه لتوسعه في مفهوم التجارة الإلكترونية، وتجاوزه المعايير التي على أساسها يمكن تعريف العمل التجاري والتي لا تخرج عن أربعة هي المضاربة، وقصد الربح، والتداول أو المقاولة، وأخيرًا الاحتراف[2].

فيدخل هذا التعريف في التجارة الإلكترونية أي نشاط دون تطلب أن تكون طبيعة هذا النشاط تجارية، كما يدخل فيها كل عمل يتعلق بالاستعلام عن السلعة أو الخدمة من قبل العميل قبل التعاقد، وكذلك كل علاقة بالعميل بعد التعاقد، والوفاء بالصفقة محل التعاقد[3].

كما عرفت بأنها قيام المتعاملين باستخدام أجهزة الحاسبات الإلكترونية وشبكة الإنترنت في إبرام الصفقات والتسوق والاتفاق على المشروعات، بحيث يصبح جهاز الحاسب الإلكتروني نافذة مفتوحة لإتمام المعاملات التجارية بسرعة فائقة.[4]

= تقرير مقدم لمركز المعلومات ودعم اتخاذ القرار، القاهرة، 2000، مشار إليه لدى د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 44، د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 7.

(1) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص35.

(2) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 7.

(3) د. حسن الماحي، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص 178.

(4) د.عصام فايد، مسئولية البنك عن فحص المستندات في الاعتماد المستندي، مرجع سابق، ص 71.

3- التعريف المخصص للتجارة الإلكترونية:

بجانب التعريفات السابقة هناك من يعرف التجارة الإلكترونية وفقا لمكوناتها أو الأطراف المشاركة فيها:

ففي المفهوم الاقتصادي: التجارة الإلكترونية هي تلك التجارة التي تقتصر على تداول السلع دون عمليات الإنتاج والتصنيع، ويتم ذلك عبر وسائل الاتصال الحديثة ومن أهمها شبكة الإنترنت العالمية، وذلك بقصد جعل المعاملات التجارية تجري بصورة تلقائية وسريعة.

وقد فرق البعض بين التجارة الإلكترونية والتجارة عبر شبكة الإنترنت، في حين أنه أصبح من المعتاد استخدام اللفظين بطريقة تبادلية، ومن الناحية العملية فإن التجارة عبر شبكة الإنترنت هي جزء من التجارة الإلكترونية[1].

ومن وجهة نظر خبراء الاتصال: تمثل التجارة الإلكترونية وسيلة من أجل إيصال المعلومات أو الخدمات أو المنتجات عبر خطوط الهاتف أو عبر الكمبيوتر أو عبر أية وسيلة تقنية[2].

ومن جانب أصحاب الأعمال التجارية: هي عملية تطبيق التقنية من أجل جعل المعاملات التجارية تسير بصورة تلقائية وسريعة[3].

وللتجارة الإلكترونية مدلول قانوني يمتد ليشمل عمليات الإنتاج والتصنيع للسلع وتداولها وذلك بقصد تحقيق الربح.

في حين أنه من ناحية تقديم الخدمات تعرف التجارة الإلكترونية بأنها

(1) د. طارق عبد العال حماد، التجارة الإلكترونية، مرجع سابق، ص 5.
(2) د. محمد الصيرفي، التجارة الإلكترونية، مؤسسة حورس الدولية، مصر، 2005، ص 148.
(3) www.uqu.edu.sa/mypage/drabid/ecommerce1.htm

أداة تعمل على تلبية رغبات الشركات والمستهلكين في خفض كلفة الخدمة ورفع كفاءتها والعمل على تسريع إيصالها، وأخيرًا فإن علماء شبكة الإنترنت يعرفونها بأنها التجارة التي تفتح المجال من أجل بيع وشراء المنتجات والخدمات والمعلومات عبر شبكة الإنترنت[1].

الفرع الثاني

تعريف التجارة الإلكترونية في الوثائق والمنظمات الدولية

تدخلت الكثير من المنظمات الدولية ذات الصلة بالتجارة الإلكترونية في محاولة لوضع تعريف ينظم عملها ويحدد إطارها، وتأتي الأمم المتحدة على رأس هذه المنظمات، فقد وضعت قانونًا نموذجيًا للتجارة الإلكترونية تسترشد به كافة الدول في تشريعاتها الداخلية، وكذلك حاولت بعض المنظمات الأخرى وضع تعريف لهذه التجارة، وكذلك هناك بعض التعريفات الواردة في بعض الوثائق الأوروبية والأمريكية والعربية، وسوف نستعرضها فيما يلي:

1- تعريف الأمم المتحدة للتجارة الإلكترونية:

وضعت لجنة الأمم المتحدة لقانون التجارة الدولية (الأونسيترال) قانونًا نموذجيًا لتيسير استخدام التجارة الإلكترونية، وليكون مقبولا لدى الدول ذات الأنظمة القانونية والاجتماعية والاقتصادية المختلفة، وليساهم في تنمية العلاقات الاقتصادية الدولية، وذلك بعد أن تزايدت نسبة التجارة الإلكترونية في التجارة الدولية، والتي تتم عن طريق التبادل الإلكتروني للبيانات وغير ذلك من وسائل الاتصال، والتي تنطوي على استخدام بدائل للأشكال الورقية للاتصال وتخزين المعلومات، وكان اعتماد اللجنة للقانون النموذجي بشأن

(1) د. عبد الفتاح مراد، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 40.

التجارة الإلكترونية في دورتها التاسعة والعشرين إيمانًا منها بأن ذلك سيساعد على نحو مهم جميع الدول في تعزيز تشريعاتها التي تنظم استخدام بدائل للأشكال الورقية للاتصال وتخزين المعلومات، وعلى صياغة هذه التشريعات في حال عدم وجودها[1].

وبالرغم من أن عنوان القانون النموذجي يشير إلى التجارة الإلكترونية، إلا أنه من الملاحظ أن هذا القانون لم يتضمن تعريفًا للتجارة الإلكترونية، وكان ذلك مقصودًا إذ إنه لدى إعداد هذا القانون قررت اللجنة أن تأخذ في الاعتبار عند التطرق إلى الموضوع المعروض عليها مفهومًا موسعًا للتبادل الإلكتروني للبيانات المتصلة بالتجارة الإلكترونية.

يشمل مفهوم التجارة الإلكترونية وفقًا للتعريف الموسع للقانون النموذجي تلك المبادلات التي تعتمد على وسائل تستند إلى استخدام التقنيات الإلكترونية، بوصفه إرسال البيانات من حاسوب إلى حاسوب بصيغة قياسية

(1) القرار الذي اتخذته الجمعية العامة للأمم المتحدة بالجلسة العامة 85 في 16 كانون الأول / ديسمبر 1996. والأونسيترال (UNCITRAL) هي الهيئة القانونية الرئيسية التابعة لمنظمة الأمم المتحدة في مجال القانون الدولي.

The core legal body of the united nations system in the field of international trade law

وهي هيئة قانونية ذات عضوية عالمية متخصصة في إصلاح القانون التجاري على النطاق العالمي منذ ما يزيد على 30 سنة.

A legal body with universal membership specializing in commercial law reform worldwide for over 30 years

ومهمة الأونسيترال هي عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية.

UNCITRAL"s business is the modernization and harmonization of rules on international business

انظر حول ذلك: http://www.uncitral.org

موحدة، وبث الرسائل الإلكترونية دون شكل محدد عن طريق شبكة الإنترنت، ولوحظ أيضًا أن مفهوم التجارة الإلكترونية قد يشمل في ظروف معينة استخدام تقنيات مثل التلكس والنسخ البرقي.(1)

وحددت المادة (1) من القانون النموذجي(2) نطاق تطبيق هذا القانون Sphere of application بنصها التالي: (ينطبق على أي نوع من المعلومات يكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية).

كما ورد بالمادة (2) والخاصة بتعريف المصطلحات Definitions for the purposes تعريفًا لرسالة البيانات Data message بأنها المعلومات التي يتم إنشاؤها أو إرسالها واستلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي(3).

وعرف القانون تبادل البيانات الإلكترونية EDI بأنه نقل المعلومات إلكترونيًا من حاسوب إلى حاسوب أو باستخدام معيار متفق عليه لتكوين المعلومات.

---

(1) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، 2006، ص 68, وفي المعنى نفسه: د.محمد سامي الشوا، الغش المعلوماتي كظاهرة مستحدثة، مرجع سابق، ص 98.

(2) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، مطبوعات الأمم المتحدة، نيويورك، 2000، ص 17.

(3) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، قوانين الأونسيترال النموذجية في مجال التجارة الإلكترونية، دار الفكر الجامعي، 2006، ص 7.

أما نظام المعلومات Information system فتم تعريفه بأنه النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها واستلامها أو تخزينها أو لتجهيزها على أي وجه آخر.

ومن الملاحظ أن صياغة القانون النموذجي تشير باستمرار إلى تقنيات الاتصال الأكثر حداثة، ومنها مثلا التبادل الإلكتروني للبيانات والبريد الإلكتروني، ولكن المقصود هو أن تطبق المبادئ التي يقوم عليها القانون النموذجي وكذلك أحكامه، في سياق تقنيات اتصال أقل تطورًا أيضًا.[1].

والملاحظ على مشروع قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية أنه لم يعرف مصطلح التجارة الإلكترونية، ولكنه اكتفى بتعريف الوسائل المستخدمة في إبرام عقود التجارة الإلكترونية، كما أن المشروع قد توسع في سرد وسائل هذه التجارة الإلكترونية بالإضافة لشبكة الإنترنت فذكر تقنية الفاكس والتلكس[2].

ويعمل مشروع القانون النموذجي بشأن التجارة الإلكترونية "Unictral" (المعتمد من الجمعية العامة للأمم المتحدة بناءً على تقرير اللجنة السادسة الخاصة بالقانون التجاري الدولي) على تيسير المعاملات التجارية[3]، ومعالجة العقود التي تبرم إلكترونيًا حيث لا توجد عقود

(1) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، مرجع سابق، ص 18.
(2) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 11.
(3) د. حسن عبد الباسط جميعي، إثبات التصرفات التي يتم إبرامها عن طريق الإنترنت، مرجع سابق، ص 83.

مكتوبة، وكذلك تكوين العقود وزمان ومكان انعقادها[1]، وقامت اللجنة التي أعدت المشروع بوضع توصية للدول بأن تأخذ مشروع القانون النموذجي للتجارة الإلكترونية بعين الاعتبار عند صياغة تشريعاتها في هذا الشأن بداية، أو عند تطوير التشريعات الوطنية القائمة، وأن تضع قواعد منظمة لاستخدام بدائل للأشكال الورقية للاتصال وتخزين البيانات[2].

2 - تعريف المنظمات الأخرى للتجارة الإلكترونية:

منظمة التعاون الاقتصادي والتنمية (OECD)[3] وضعت للتجارة الإلكترونية تعريفًا يشمل جميع أشكال المعلومات التجارية التي تتم بين الشركات أو الأفراد، والتي تقوم على أساس التبادل الإلكتروني للبيانات سواء أكانت مكتوبة أو مرئية أو مسموعة، هذا بالإضافة إلى شموله الآثار المترتبة على عملية تبادل البيانات والمعلومات التجارية إلكترونيًا، ومدى تأثيرها على المؤسسات والعمليات التي تدعم وتحكم الأنشطة التجارية المختلفة.

وعرفت منظمة التجارة العالمية (WTO)[4] التجارة الإلكترونية بأنها التجارة التي تغطي الإنتاج، الترويج، البيع والتوزيع للمنتجات من خلال شبكة الاتصالات وأدواتها مثل التليفون، الفاكس، والتبادل الإلكتروني للمعلومات، والبريد الإلكتروني، وشبكة الإنترنت من خلال (WWW)

(1) د. محمد السعيد رشدي، حجية وسائل الاتصال الحديثة في الإثبات، مرجع سابق، ص 64.

(2) د. إبراهيم أحمد، تقرير عن الجوانب القانونية للتجارة الإلكترونية في مصر، تقرير مقدم لمركز المعلومات ودعم اتخاذ القرار، مرجع سابق، ص 593.

(3) OECD = Organization for Economic Cooperation and Development

(4) WTO = World Trade Organization

.World Wide Web

واعتبرت منظمة التجارة العالمية التجارة الإلكترونية - من تعريفها السابق بيانه - أنها مجموعة متكاملة من العمليات تشمل تأسيس الروابط التجارية، وعقد الصفقات، وتوزيع وتسويق وبيع المنتجات عبر وسائل إلكترونية[1].

وقد انعقد المؤتمر الوزاري لمنظمة التجارة العالمية في 15 مايو 1998، وجاءت نتائجه وتوصياته تلقي الضوء على أهمية التجارة الإلكترونية وتطورها، وضرورة الإصلاح التشريعي لإيجاد نظام قانوني موحد يشجع التجارة الإلكترونية، ويعمل على بث الثقة والطمأنينة لاستخدام التوقيعات الإلكترونية كبديل عن التوقيعات المكتوبة، والاهتمام التشريعي بهذا الموضوع، ونشر الوعي بما تشتمل عليه التجارة الإلكترونية، وبأهميتها المتزايدة في الصفقات التجارية[2].

---

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 6.

(2) وتنص توصيات هذا المؤتمر على ما يلي:

أ- نظرًا لأن التجارة الإلكترونية لا تتقيد بالحدود الوطنية، فإن تطورها يتطلب من جميع المهتمين بالتجارة العالمية من حكومات ومنظمات حكومية وغير حكومية ذات صلة وقطاع خاص الاهتمام بها وتنميتها، وعلى ذلك فإن الجهود مستمرة على المستويين المحلي والدولي لخلق بيئة قانونية وفنية مناسبة للتجارة الإلكترونية.

ب- لن تكتب لهذه التجارة التطور والانتعاش إلا بتمتع التجارة بقدر كبير من الثقة والأمن في مسائل عديدة مثل صحة الصفقات، وسلامة المعلومات، ومصداقية آليات الصفقات، والحق في الرجوع في حالة الخطأ أو الإهمال، وتأثير الصفقات على الأطراف الأخرى البريئة.

ج- دلت الأبحاث التي أجرتها عدة منظمات مثل Micitral ECF ولجنة المجتمعات الأوروبية على أن القوانين القائمة والتشريعات المتعلقة بالصفقات التجارية غير=

3 - تعريف التجارة الإلكترونية في الوثائق الأوروبية والأمريكية والعربية:

تعرف اللجنة الأوروبية(1) التجارة الإلكترونية EC بأنها أداء الأعمال إلكترونيًا، حيث تقوم على أساس التبادل الإلكتروني للبيانات، مكتوبة كانت

= ملائمة للتجارة الإلكترونية، ومن المحتمل أن تخلق شكوكًا في صحتها وسريانها، ومن المسلم به أن المزايا الفعالة للتجارة الإلكترونية لا يمكن أن تتحقق بدون وجود إطار قانوني مناسب.

د- ستعمل ثورة المعلومات الناتجة عن شبكة الإنترنت والنمو السريع للتجارة الإلكترونية على التأثير بشكل مباشر على التجارة بين الدول المتقدمة والنامية، والمقترح أن تقوم الدول النامية والدول الأقل تطورا بالتفكير في إيجاد بيئة قانونية وتنظيمية للتجارة الإلكترونية.

هـ- أما عن الإصلاح التشريعي، فإنه قد يكون من الضروري الاستفادة من مخزون القوانين واللوائح الخاصة بالتجارة الإلكترونية، ومن الممكن إجراء التعديلات الضرورية التي تفي بمتطلبات التجارة الإلكترونية، ولتجنب خطر إيجاد نظام قانوني غير موحد قد يضر ولا يشجع التجارة الإلكترونية قد يكون من المفيد النصح باتباع القوانين العالمية إلى أقصى حد ممكن، ومن ذلك قانون unictral للتجارة الإلكترونية، لذلك قد يكون ضروريا أن تأخذ الدول النامية بأحدث التطورات في الاجتماعات العالمية المتعددة والتي تؤثر في التجارة الإلكترونية.

و- المجال الرئيسي الذي يحتاج لاهتمام تشريعي هو موضوع التوقيعات الإلكترونية كالتوقيعات الرقمية ووسائل التصديق الإلكتروني الأخرى، إذ إن تجارب الشبكات المفتوحة والصفقات الكبرى تتطلب بلا شك استخدام أسلوب توقيعي إلكتروني آمن مثل التوقيع الرقمي، ورغم وجود تكنولوجيات أخرى في طريقها إلى الظهور إلا أن تكنولوجيا التوقيع الرقمي معروفة على نطاق واسع الآن، وهي حاليا محط اهتمام المشرعين في عدة دول.

انظر في توصيات هذا المؤتمر: د. محمد السعيد رشدي، حجية وسائل الاتصال الحديثة، مرجع سابق، ص 65.

(1) EC= European Commission

أو مرئية أو مسموعة، كما أنها تتضمن العديد من الأنشطة التجارية الخاصة بتبادل السلع والخدمات، وإتمام عمليات البيع والشراء والتسليم بالنسبة للمحتويات الرقمية والتحويلات الإلكترونية للأموال والفواتير الإلكترونية والمزادات التجارية، وعمليات التسويق وخدمات ما بعد البيع، وهي تشمل كلا من السلع والخدمات، وكذلك الأنشطة التقليدية وغير التقليدية[1].

قصر التوجيه الأوروبي الصادر في 20 مايو 1997 والمتعلق بحماية المستهلك في العقود المبرمة عن بُعد في مادته الثانية تعريفه على العقد الإلكتروني، فعرفه بأنه هو كل عقد يتعلق بالسلع أو الخدمات يتم بين مورد ومستهلك عن بُعد، أو تقديم الخدمات التي ينظمها المورد والذي يتم باستخدام واحدة أو أكثر من وسائل الاتصال الإلكترونية لإتمام العقد[2].

كما عرف التوجيه المشار إليه تقنية الاتصال عن بُعد بأنها كل وسيلة - دون وجود مادي ولحظي للمورد والمستهلك - يمكن أن تستخدم لإبرام العقد بين طرفيه[3].

ثم جرت محاولات أخرى في أوروبا، لإيجاد إطار عام تلتزم به دول المجموعة الأوروبية أثناء إصدار تشريعاتها الداخلية المتعلقة بتعديل قواعد الإثبات بما يتماشى مع متطلبات التجارة الإلكترونية، وتم تحديد ثلاثة محاور في هذا الشأن: الأول بشأن الأثر القانوني للتوقيع الإلكتروني، والثاني يتعلق باعتماد هذا التوقيع والاعتراف المتبادل بين الدول الأعضاء وتحديد المواصفات التي يتم على أساسها اعتماد التوقيع الإلكتروني، والثالث

(1) د. السيد أحمد عبد الخالق، التجارة الإلكترونية والعولمة، المنظمة العربية للتنمية الإدارية، 2006، ص 34.
(2) www.tashreaat.com/view_studies2.asp?id=288std_id=66
(3) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص14.

يتعلق بتحديد التزامات الجهة القائمة على خدمة اعتماد التوقيع الإلكتروني.

وتم تشكيل لجنة لهذا الغرض، ووضعت اللجنة مشروع الإطار المنوط بها إعداده، وفي30 نوفمبر 1999 تم إقرار هذا المشروع وأصبح يسمى باسم التوجيه الأوروبي بشأن المحررات الموقعة إلكترونيًا.

ثم صدر توجيه آخر عن البرلمان الأوروبي تحت رقم 2000-31 في 8 يونيو 2000[1] في شأن بعض الجوانب القانونية لخدمات شركة المعلومات وبصفة خاصة التجارة الإلكترونية في السوق المحلي، فقد عرف الاتصال التجاري بأنه كل شكل من أشكال الاتصال يستهدف تسويق بضائع أو خدمات بصورة مباشرة أو غير مباشرة، مشروع أو منظمة أو شخص يباشر نشاطًا تجاريًا أو صناعيا.[2].

والواضح أن هذا التوجيه قد صدر عاما وشاملا لموضوع التجارة الإلكترونية وأشخاصها، على خلاف التوجيه الأول الذي خص التعاقد عن بعد المتعلق بالبضائع أو الخدمات، في حين أن التوجيه الثاني تحدث عن تسويق البضائع والخدمات والأنشطة التجارية أو الصناعية أو الحرفية أو المهنية بصورة منتظمة.

وتضمن التوجيه إشارة للدول الأعضاء بتعديل تشريعاتها كي تستوعب التجارة الإلكترونية وألا تؤثر عليها بصورة سلبية بأن تحد من أثرها أو فاعليتها لمجرد أنها تتم بتقنية إلكترونية[3].

---

(1) **Directive 2000/31/EC of the European Parliament and of the Council، of 8 June 2000، on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).**

(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص15.

(3) د. عبد الفتاح مراد، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 37.

أما في الوثائق الحكومية الأمريكية فقد عرفت التجارة الإلكترونية بأنها الاستعمال الأمثل لكل أنواع تكنولوجيا الاتصالات المتاحة من أجل تنمية النشاط التجاري للمشروعات[1].

وقد عرفتها نشرة المؤسسة العربية لضمان الاستثمار بأنها "التجارة التي تتم باستخدام التقنيات التي وفرتها ثورة المعلومات والاتصالات وشبكة الإنترنت، عبر التبادل الإلكتروني لبيانات متجاوزة عنصري الزمن والمكان، وتغطي قطاعات عديدة من بائعي التجزئة إلى الوسطاء الماليين، وتضع قواعد جديدة لعمليات البيع والتسجيل والتسليم وغير ذلك"[2].

ومن هذا التعريف يتضح أن التجارة الإلكترونية تغطي في الغالب الأعم قطاعات من بائعي التجزئة والوسطاء الماليين، وهي تتيح للمتعاملين إمكانية الوصول إلى جميع أسواق العالم في وقت واحد وبأقل النفقات[3] للوقوف

---

(1) استخلص البعض هذا التعريف من وثيقتين: الأولى هي الوثيقة الرسمية الصادرة في 22 فبراير 1993 بعنوان (تكنولوجيا النمو الاقتصادي الأمريكي، اتجاه جديد في بناء القوة الاقتصادية) والتي أعدها نائب الرئيس الأمريكي آل جور واعتمدها الرئيس، والتي أشارت إلى الدور الأساسي الذي تحتله شبكات المعلومات في مستقبل التجارة والمجتمع في أمريكا، والثانية أعدها فريق العمل الفيدرالي المختص بالتجارة الإلكترونية في 29 أبريل 1994 بعنوان: Streamlining Procurement Through Electronic Commerce والخاصة باستخدام شبكات المعلومات في التجارة الإلكترونية.
د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص36.

(2) د. محمد السعيد رشدي، حجية وسائل الاتصال الحديثة، مرجع سابق، ص 62.

(3) د. إبراهيم أحمد إبراهيم، التجارة الإلكترونية والملكية الفكرية، مرجع سابق، ص62.
"P.C. Magazine"، الطبعة العربية، السنة السادسة، العدد الثاني، مارس / آذار 2000، ص18.

على السلع والخدمات التي يرغبون فيها وأسعارها، وإمكانية المفاضلة بين أكثر من عرض لها، سواء من حيث الجودة أو من حيث الثمن، وإجراء حوارات بين البائعين والمشترين بغرض إبرام صفقات يتم الاتفاق فيها على نوع السلعة أو الخدمة وكميتها وكيفية تسليمها وطريقة الوفاء بالثمن، بعيدًا عن الطرق التقليدية التي كانت سائدة من قبل في إبرام مثل هذه الاتفاقيات وعقد تلك الصفقات.

ويمكن للطرف الراغب في تسويق ما لديه من سلع ومنتجات وخدمات تسويقها عن طريق موقع، وبريد إلكتروني، وعنوان على شبكة الإنترنت أو صفحة يعرض فيها إمكانياته وفقًا لأحدث فنون العرض المقدمة، ويمكن تقسيم ما يعرض على شبكة الإنترنت من سلع وخدمات إلى قسمين، الأول يمكن تسليمه إلكترونيًا مثل الخدمات التعليمية والطبية والمحاسبية والثقافية والمصرفية، والثاني لا يمكن تسليمه إلكترونيًا مثل الحاجة لنقل بعض السلع أو الخدمات إلى من تعاقد على شرائها أو تجربتها أو تشغيلها.

والفكرة الرئيسية للتجارة الإلكترونية والتي بموجبها يتمكن البائعون من تسويق ما لديهم من سلع ومنتجات، ويتمكن المشترون من الوصول إليهم بأقل النفقات في وقت واحد، تدور حول تجمع البائعين في معرض أو مراكز تجارية أو فترينات تجارية افتراضية، وذلك من أجل عرض بضائعهم.

وتنقسم المراكز التجارية الافتراضية إلى قسمين: أولهما يمكن الدخول إليه دون حاجة لإجراءات معينة، ولكنه يسمح للزائرين بالاطلاع فقط، بحيث يتمكن الزائر من التجول في المراكز من أجل التعرف على السلع والمنتجات والخدمات المعروضة دون أن يتمكن من شرائها، ولكي يتمكن من الشراء يكون من المتعين عليه أن يدخل إلى القسم الثاني الذي لن يتمكن

من الدخول إليه إلا بعد اتباع إجراءات معينة تستهدف التحقق من شخصية الزائر وتسجيله، ويتم ذلك بقيام الزائر بذكر رقم بطاقته الائتمانية من أجل تيسير الوفاء.

كما يجب أن يتبنى توقيعًا رقميًا ذا شفرة خاصة لاعتماد التصرفات التي يبرمها، فإذا تمت هذه الإجراءات كان بإمكان الزائر الدخول إلى صفحات البيع لمختلف المحلات التجارية التي يتكون منها المركز التجاري، وأن يتعاقد على المنتجات أو الخدمات التي يرغب في شرائها، ويجب عليه بعد ذلك أن يقدم نفسه مستخدمًا الكود الخاص به كلما أراد الدخول إلى هذا المركز، مع ملاحظة أنه إذا دخله فإنه يستطيع الدخول بحرية إلى المحلات المشاركة فيه دون حاجة للتحقق منه عند دخول كل منها، فإذا دخل الزائر أحد المحلات فإنه يجد نفسه أوتوماتيكيًا أمام مجموعة من الصفحات التي تتضمن شروط التعاقد والتي يكون بوسعه أن يقبلها أو أن يرفضها[1].

وفي النهاية فإن مصطلح التجارة الإلكترونية أصبح دارجًا ومتداولا بكثرة لدى جميع القطاعات سواء أكانت اقتصادية أم قانونية أم بين عموم الناس سواء كانوا مستخدمي شبكة الإنترنت أم في الحياة العامة.

الفرع الثالث

تعريف القوانين الوطنية للتجارة الإلكترونية

نظمت الكثير من القوانين على مستوى العالم التجارة الإلكترونية، وحاول بعضها وضع تعريف لها، واكتفى البعض الآخر بالتعريف التقليدي

(1) Lionel costs:"Aperçu sur le droit du commerce électronique aux Etats Unis"،droit et patrimoine، N 55، décembe 1997 p. 67.

وفي المعنى ذاته: د. أسامة أبو الحسن مجاهد، مرجع سابق، ص 13.

للتجارة مضيفًا إليها الوسيلة الإلكترونية التي تباشر بها، وسنتعرض لبعض هذه التعريفات سواء في بعض القوانين الأوروبية أو العربية، خصوصًا تلك التي نظمت التجارة الإلكترونية أو تتعامل بها.

1 - في القوانين الأوروبية

في فرنسا عرف القانون الفرنسي العمل التجاري ولم يعرف التجارة الإلكترونية، فالتجارة هي ممارسة العمل التجاري على وجه الاعتياد، وبالتالي لن تكون التجارة الإلكترونية سوى ممارسة الأعمال التجارية التي نصت عليها المادة (632) من تقنين التجارة بوسيلة إلكترونية على سبيل الاعتياد، ومن ثم يمكن القول بأن التجارة الإلكترونية لا تختلف كثيرًا عن التجارة بصفة عامة من حسب مضمونها ومحترفوها[1]، أما وجه الخصوصية فيها فيتمثل في وسائل مباشرتها، وبصفة خاصة الطريقة التي تنعقد بها العقود وطريقة تنفيذها[2].

وقد عرفت مجموعة العمل المشكلة برئاسة وزير الاقتصاد الفرنسي[3] التجارة الإلكترونية بأنها مجموعة المعاملات الرقمية المرتبطة بأنشطة تجارية، بين المشروعات بعضها البعض وبين المشروعات والأفراد، وبين المشروعات والإدارة[4].

وأعطت الجمعية الفرنسية للتليماتيك والمالتيميديا ((AFTELللتجارة

---

(1) Christiana Feral،Schuhl، Cyber Droit le droit 'a l'epreuve de l'internet، 3 e'dition 2001، p387.

(2) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص 35.

(3) السيد لورنتز Lorentz وزير الاقتصاد الفرنسي، وتم تشكيل هذه المجموعة في يناير 1998.

(4) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص12.

الإلكترونية تعريفين[1]:

التعريف الأول ضيق حيث عرفتها بأنها "" مجموعة من المعاملات التجارية التى يتم الشراء فيها عن طريق وسائل الاتصال "" وبالتالي فإن التجارة الإلكترونية تشمل عملية تلقى الطلب، وكذلك الشراء مع السداد، وتتعلق بصورة أكبر بالعمليات المتعلقة بشراء السلع عن تلك المتعلقة بالخدمات، سواء اتخذت الأخيرة شكل المعلومات أو شكل الألعاب.

والتعريف الثاني واسع حيث جعلها تشمل مجموعة الاستعمالات التجارية لوسائل الاتصال، ومنها قيام المشروع فقط بعرض بضاعته بحيث يتم طلب البضاعة بالطرق التقليدية.[2]

ونرى أن التعريف الفرنسي توسع في مفهوم التجارة الإلكترونية ليشمل كافة أوجه وصور النشاط الإلكتروني للتجارة المتصور ما بين الأفراد والمشروعات والإدارة، ويرى جانب من الفقه أن هذا التوسع له ما يبرره، إذ إن المعاملات الرقمية - وحسبما أشارت اللجنة المذكورة - قد ترتبط بأنشطة تجارية تشمل أنشطة البنوك باعتبار أنها تساهم في إبرام المعاملات التجارية عن طريق أنظمة السداد، وتشمل هذه التجارة أيضًا أنشطة تبادل المعلومات والتعاملات المتعلقة بالبضائع والتجهيزات أو بضائع الاستهلاك التجاري، وكذلك الخدمات كخدمات المعلومات المالية والقانونية[3].

ويخضع نشاط التجارة الإلكترونية لنصوص التشريع الفرنسي الصادر

(1) د. حمد الله محمد حمد الله، مختارات من قانون الاستهلاك الفرنسي، دار النهضة العربية، القاهرة، 2000، ص 91.

(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، 2001، ص 18.

(3) المرجع السابق، ص13.

في 6 ينـاير 1978 والخـاص بالمعلوماتيـة والحريـات، والقـانون رقـم (2000/230) والمرسـوم رقـم (2001/741) والقانون رقم (2001/1062) المتعلق بالسلامة اليومية، بالإضافة إلى قـانون التوقيـع الإلكـتروني رقـم (2000/230)، كـما صـدر في 21 يونيـو 2004 قـانون يتعلـق بالثقـة في الاقتصـاد الرقمي، ويدخل في نطاق معالجة البيانات إلكترونيًا، ويعد تقديم العروض مـن خـلال الشـبكات من قبيل خدمات الاتصالات المرئية المسموعة بالمعنى المقصود في القانون الصـادر في30 ديسـمبر 1986 بشأن حرية الاتصالات، والذي عرف الاتصـالات عـن بعـد بأنهـا (كـل انتقـال أو إرسـال أو استقبال لرموز أو إشارات أو كتابة أو صور أو أصوات أو معلومات أيًا كانـت طبيعتهـا، بواسـطة ألياف بصرية أو كهرباء لاسلكية أو أية أنظمة إلكترونية مغناطيسية أخرى)[1].

وفي إيطاليا أصدر المشرع الإيطالي القرار بقانون في شأن التجارة الإلكترونية عام 1999 فقـنن اتجاه البرلمان والمجلس الأوروبي رقم 7/97 فيما يتعلق بشأن حماية المستهلكين في مجـال العقـود عن بعد، رغم ما يراه جانب من الفقه الإيطالي من أن التجارة الإلكترونية تختلف عن البيـع عـن بعد؛ لأن المستهلك في التجارة الإلكترونية لا يقف موقفًا سلبيًا كما هو الشأن بالنسبة للمسـتهلك في البيع عن بعد، حيث يساهم بدور إيجابي مباشر في إعداد العقد، ومع ذلـك يـرى جانـب مـن الفقه أن الاختلاف بين التجارة الإلكترونية والعقود عن بعد ليس بكبـير إذا أخـذنا في الاعتبـار أن المشتري لا يطلع مباشرة على المال محل العقد[2].

(1) Christiana Feral.Schuhl، Cyber Droit le droit 'a l'epreuve de l'internet- OP، CIT، p 389.
(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص13.

والواقع أن المستهلك في التجارة الإلكترونية معني بها وإن لم يكن طرفًا فيها غالبًا، فهو في النهاية مستهلك للخدمة أو السلعة التي تسوق عن طريق التجارة الإلكترونية[1].

وفي مشروع قانون التجارة الإلكترونية في دوقية لوكسمبرج عرف في مادته الأولى المخصصة للتعريفات التجارة الإلكترونية بأنها: "كل استعمال لوسيلة من وسائل الاتصال الإلكترونية لتجارة السلع والخدمات باستثناء العقود المبرمة بطريق اتصال تليفوني شفهي أو باستخدام التصوير". ومن الملاحظ أن هذا التعريف اعتبر التجارة إلكترونية إذا استعملت فيها وسيلة من وسائل الاتصال الإلكترونية، وأنها تنطوي على نوعين هما تجارة السلع وتجارة الخدمات، إلا أن القانون الصادر بتاريخ 12 يوليو 2000 خلا من أي تعريف للتجارة الإلكترونية[2].

2 - في القوانين العربية:

يعد القانون التونسي رقم 83 لسنة 2000 بشأن المبادلات والتجارة الإلكترونية أول قانون عربي يصدر بشأن التجارة الإلكترونية[3]، وقد أورد في الفصل الثاني من الباب الأول تعريفًا للمبادلات الإلكترونية، وللتجارة الإلكترونية، حيث نص على أنه يقصد بالمصطلحات الآتية في مفهوم القانون ما يلي:

المبادلات الإلكترونية: المبادلات التي تتم باستعمال الوثائق الإلكترونية.

التجارة الإلكترونية: العمليات التجارية التي تتم عبر المبادلات الإلكترونية.

(1) د. عبد الفتاح مراد، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 34.
(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص6.
(3) قانون المبادلات والتجارة الإلكترونية التونسي الصادر بتاريخ 9 أغسطس 2000.

من هذا التعريف يتضح لنا أن القانون التونسي عرف التجارة الإلكترونية بأنها أي عملية تجارية، سواء أكان موضوعها سلعة أو خدمة أو أداء عمل وذلك عن طريق المبادلات الإلكترونية، لأن أي عملية تجارية هي مبادلة ما بين سلعة وثمنها، أو خدمة وقيمتها، أو أداء عمل ومقابله، شرط أن يتم ذلك بوثيقة إلكترونية، أي وثيقة تمت صياغتها بطريقة إلكترونية[1]، كما يتضح لنا من هذا التعريف أن القانون التونسي لم يحدد الوسائل التي يتم بها التعاقد عن بعد؛ على اعتبار أن هذه الوسائل في تطور مستمر ومن الصعب حصرها في تقنيات معينة.

وفي دولة الإمارات العربية المتحدة كان السبق لإمارة دبي عندما أصدرت القانون المحلي رقم 1 لسنة 2000 بشأن منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام، والذي نص في مادته الثانية على أن التجارة الإلكترونية هي الأعمال المنفذة بالوسائط الإلكترونية وبشكل خاص شبكة الإنترنت، كما أصدرت الإمارة بتاريخ 12 فبراير 2002 قانون المعاملات والتجارة الإلكترونية رقم 2 لسنة 2002[2] ونص أيضًا في المادة الثانية من الفصل الأول الخاص بالتعريفات على أن:

- المراسلة الإلكترونية: إرسال واستلام الرسائل الإلكترونية.
- الرسالة الإلكترونية: معلومات إلكترونية ترسل أو تستلم بوسائل إلكترونية أيًا كانت وسيلة استخراجها في المكان المستلمة فيه.
- التجارة الإلكترونية: المعاملات التجارية التي تباشر بواسطة المراسلات الإلكترونية.
- المعاملات الإلكترونية: أي تعامل أو عقد أو اتفاقية يتم إبرامها أو

(1) د. عبد الفتاح مراد، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص42.
(2) يقتصر تطبيق هذا القانون على إمارة دبي فقط باعتبار أنه قانون محلي.

تنفيذها بشكل كلي أو جزئي بواسطة المراسلات الإلكترونية.

والملاحظ على هذين التعريفين أن الأول توسع في التجارة الإلكترونية عندما أدخل فيها جميع الأعمال المنفذة بالوسائط الإلكترونية، الأمر الذي من شأنه دخول أعمال غير تجارية في موضوع التجارة الإلكترونية، ومن ناحية أخرى نرى أن هذا التعريف حاول التركيز بشكل خاص على شبكة الإنترنت دون إهمال للوسائط الإلكترونية الأخرى.

أما التعريف الآخر فقد قصر على المعاملات التجارية والتي تباشر عن طريق إرسال واستلام تلك المعلومات الإلكترونية، والتي ترسل أو تستلم بوسائل إلكترونية أيًا كانت وسيلة استخراجها في المكان المستلمة فيه، وهنا اقترب هذا التعريف من قانون الأونسيترال النموذجي السابق بيانه عندما أخذ بالمفهوم الواسع للتبادل الإلكتروني للبيانات[1].

وفي 3 يناير 2006 صدر القانون الاتحادي رقم 1 لسنة 2006 بشأن المعاملات والتجارة الإلكترونية والخاص بدولة الإمارات العربية المتحدة ونص في الفصل الأول الخاص بالتعريفات في المادة (1) على التعريف السابق بيانه والوارد في قانون التجارة الإلكترونية الخاص بإمارة دبي، وذلك على اعتبار أن القانون الاتحادي يكاد أن يكون صورة مطابقة لقانون التجارة الإلكترونية الخاص بإمارة دبي كون أن لها السبق في هذا المجال، وأن قانونها صدر قبل أربع سنوات من صدور القانون الاتحادي.

ومن القوانين العربية الأخرى قانون المعاملات الإلكترونية الأردني

(1) د. نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، مايو 2000، ص3.

رقم 85 لسنة 2001[1]، حيث عرف المعاملات الإلكترونية في مادته الثانية بأنها المعاملات التي تنفذ بوسائل إلكترونية.

وهناك العديد من الدول العربية التي أعدت مشروعات للتجارة الإلكترونية، منها مشروع قانون المبادلات والتجارة الإلكترونية الفلسطيني، فقد نص في الفصل الأول الخاص بالتعريفات والأحكام العامة في المادة الأولى على أنه: في تطبيق أحكام هذا القانون يكون للكلمات والعبارات التالية المعاني المخصصة لها أدناه ما لم تدل القرينة على خلاف ذلك:

- المبادلات الإلكترونية: المبادلات التي تتم باستعمال رسائل البيانات.
- رسالة البيانات: المعلومات التي يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل مشابهة، ويشمل ذلك تبادل البيانات الإلكترونية، أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي.
- التجارة الإلكترونية: كل معاملة تجارية تتم عن بعد باستخدام وسيلة إلكترونية.

وفي دولة الكويت يوجد مشروع قانون التجارة الإلكترونية والذي عرف هذه التجارة بأنها المعاملات التجارية التي تباشر بوسائط إلكترونية، وعرف المعاملات الإلكترونية بأنها أي تعامل أو تعاقد أو اتفاق يتم إبرامه أو تنفيذه بشكل كلي أو جزئي بواسطة وسائل إلكترونية.

وفي جمهورية مصر العربية عرف مشروع قانون التجارة الإلكترونية في مادته الأولى الخاصة بالتعريفات التجارة الإلكترونية بأنها كل معاملة تجارية تتم عن بعد باستخدام وسيلة إلكترونية[2].

(1) المنشور على الصفحة 6010 من عدد الجريدة الرسمية رقم 4524 بتاريخ 2001/12/31.
(2) د مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص16.

وعرف مشروع قانون تكنولوجيا المعلومات اللبناني التجارة الإلكترونية بأنها نشاط اقتصادي يتم عن بعد بوسيلة إلكترونية لتأمين خدمة أو سلعة.

كما عرفها مشروع القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية بأنها المعاملات التجارية التي تباشر بواسطة وسائل إلكترونية، وعرف المعاملات الإلكترونية بأنها أي تعامل أو تعاقد أو اتفاق يتم إبرامه أو تنفيذه بشكل كلي أو جزئي بواسطة وسائل إلكترونية.

وبالبحث وجدنا أن كافة التعريفات تتوافق مع المفهوم اللغوي لمصطلح التجارة الإلكترونية الذي يتكون من قسمين: الأول التجارة وهي مأخوذة من فعل تجر وهو يعني ممارسة البيع والشراء، وهي حرفة التاجر الذي يمارس الأعمال التجارية على وجه الاحتراف، وفي الاصطلاح عند الاقتصاديين: هي مبادلة السلع والخدمات بهدف إشباع الحاجات الإنسانية المتعددة، فإذا تمت عملية المبادلة بين المقيمين داخل الدولة الواحدة أطلق عليها التجارة الداخلية، وإذا تمت بين المقيمين في عدة دول، أو بين دولة ودولة أخرى أطلق عليها التجارة الخارجية، أو التجارة الدولية International Trade.

أما القسم الثاني وهو الإلكترونية فهو نوع من التوصيف لمجال أداء النشاط المحدد في القسم الأول، ويقصد به هنا أداء النشاط التجاري باستخدام الوسائط والأساليب الإلكترونية ووسائل الاتصال الحديثة المعالجة إلكترونيا، وتعد شبكة الإنترنت من أهم هذه الوسائط[1].

وفي النهاية وباستعراضنا لكافة التعريفات فإننا نستطيع القول بأنه يقصد بالتجارة الإلكترونية تلك التجارة التي تشمل كافة الأنشطة التجارية للمنتجات والخدمات التي تتم إلكترونيا باستخدام تكنولوجيا المعلومات وعبر شبكة

(1) رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص13.

اتصال وباستخدام التبادل الالكتروني للبيانات لتنفيذ العمليات التجارية, سواء أكان من المنتجين أو الموزعين أو الوسطاء, من ناحية والمستهلك من ناحية أخرى, أو بين المهنيين, وكذلك بين الأفراد وبعضهم البعض, مع عدم التواجد المادي لطرفي العقد في ذات المكان, وتشمل هذه التعاملات التجارة الخارجية والداخلية, بالإضافة إلى إمكانية قيام التجارة الإلكترونية بوظائف جديدة في عمليات التبادل التجاري مثل الإعلان والتسويق والمفاوضات والتبادل لبعض السلع والخدمات.

وترتيبا على ما سبق نتوصل إلى أن التجارة الالكترونية صورة من صور التعاقد عن بعد والتي أدت إلى وجود مشاكل عملية وقانونية تتعلق بفروع القانون المختلفة وبصفة خاصة في مجالات القانون المدني والقانون التجاري والقانون الدولي الخاص والقانون الجنائي وقواعد وإجراءات الإثبات.([1])

ويلاحظ أننا في التعريف السابق لم نقصر الأنشطة التجارية على تلك التي تتم عبر شبكة الإنترنت فقط، إذ إن هناك شبكات أخرى مماثلة لشبكة الإنترنت مثل شبكة BIT NET، وشبكة UU NET، يمكن أن تقدم أسواقًا جديدة للتجار والمستهلكين الذين يرغبون في التعاقد الإلكتروني، وإن كانت شبكة الإنترنت أشهر وأكبر الشبكات حتى الآن.

(1) د. مدحت رمضان - الحماية الجنائية للتجارة الالكترونية - المرجع السابق - ص21.

المطلب الثالث

أشكال التجارة الإلكترونية

ينظر للتجارة الإلكترونية على أنها مفهوم متعدد الأبعاد، ويمكن أن يتم من خلال أكثر من شكل، ولعل أهم أشكال التجارة الإلكترونية ما يتم بين المنشآت التجارية من جهة وبين تلك المنشآت والمستهلكين من جهة أخرى، ونتناول أشكال التجارة الإلكترونية على النحو التالي:

1) التجارة الإلكترونية بين منشأة تجارية ومنشأة تجارية Business to Business:

ويرمز لها بالرمز(B to B)، ويقصد بهذا النوع أن تتم المعاملات التجارية بين التجار بعضهم البعض، سواء أكانوا أشخاصًا أو شركات، باستخدام شبكة الاتصالات وتكنولوجيا المعلومات لإنجاز الصفقات فيما بينها، بتبادل الوثائق إلكترونيًا لتقديم طلبات الشراء إلى الموردين وتسلم الفواتير وكذلك القيام بعملية الدفع، وهذا الشكل هو أكثر أنواع التجارة الإلكترونية شيوعًا في الوقت الحالي، سواء داخل الدولة على المستوى الوطني، أو بين الدول بعضها البعض على المستوى الدولي، وتؤدي هذه الصورة إلى خفض التكاليف وزيادة كفاءة العملية التجارية وتحقيق معدل أعلى في الأرباح[1].

وتمثل هذه الصورة للتجارة الإلكترونية ما يربو على 90% من التعاملات الإلكترونية الأكثر قيمة وأهمية اقتصادية في العالم، فتتضمن سلعًا مثل الصلب والكيماويات، وتشمل أيضًا التحالفات بين شركات صناعة السيارات والطيران والفضاء، وهو مجال يسهل نسبيًا تنظيمه من الوجهة

(1) رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص 30.

القانونية المدنية فلا يستلزم تطويرًا تشريعيًا ضخمًا، فالعقد شريعة المتعاقدين, مع إعادة النظر في بعض القواعد المدنية التقليدية خاصة تلك المتعلقة بالإثبات.

2) التجارة الإلكترونية بين منشأة تجارية ومستهلك Business to Customer:

ويرمز لها اختصارًا بالرمز (B to C)، ويطلق على هذا الشكل كذلك اسم التسوق الإلكتروني، أو تجارة التجزئة الإلكترونية، لأن الصفقة تتم مع المستهلك، فتقوم المنشآت بعرض منتجاتها على متاجر إلكترونية افتراضية على شبكة الويب، وتعقد الصفقات من العملاء الراغبين في شراء السلع والخدمات، ويتم الدفع بطرق مختلفة أكثرها شيوعًا عن طريق استخدام بطاقات الائتمان أو الشيكات الإلكترونية أو نقدًا عند التسليم، كما أن هذا الشكل يستخدم من قبل المنشأة التجارية للوصول إلى أسواق جديدة.

ومن أمثلتها ذلك المجمع التجاري الإلكتروني الموجود في سريلانكا الذي يعرض مختلف أنواع الشاي والملابس والأحجار الكريمة التي يشتهر بها هذا البلد[1]، والتي يتكون جمهورها من مختلف الدول، وتتمكن من اجتذاب أكبر عدد ممكن من الزائرين وذلك بعرضها تشكيلة واسعة من المنتجات والخدمات، وتقديم المعلومات عن الشركات المنتجة لها وبلد المنشأ والمدة التي يستطيع فيها المستهلك الرجوع عن القبول، وغير ذلك من المعلومات مما تفرضه الاتفاقيات الدولية والقوانين الوطنية لحماية المستهلك.

---

(1) د. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005، ص 21.

3) **التجـارة الإلكترونيـة بـين منشـأة تجاريـة والإدارة الحكوميـة Business to Administration**

ويرمز لها (B to A)، وهي تغطي جميع التعاملات التي تتم بين وحدات الأعمال والإدارات الحكومية، مثال ذلك ما تقوم به الولايات المتحدة وكندا مـن عـرض الإجـراءات واللـوائح ونمـاذج المعاملات على شبكة الإنترنت بحيث تستطيع الشركات أن تطلـع عليهـا بطريقـة إلكترونيـة، وأن تقوم بإجراء المعاملة إلكترونيًا دون حاجة للتعامل مع مكتب حكومي[1].

4) **التجـارة الإلكترونيـة بـين المسـتهلكين والإدارة الحكوميـة Administration to Customer:**

ويرمز لها (A to C)، بدأ هذا الشكل في الانتشار في الآونة الأخيرة في كثير من الدول، ومثال ذلك دفع الضرائب إلكترونيًا [2]، واستخراج ترخيص القيادة، وتجديد تراخيص المركبات.

5) **التجارة الإلكترونية من مستهلك إلى مستهلك Customer to Customer:**

وهو ما يعبر عنه بالرمز (C to C)، وقـد ظهـر هـذا الشـكل مـع انتشـار اسـتخدام شـبكة الإنترنت وظهور التقنيات الحديثة، والنوع الرئيسي لهذا الشكل هو المعاملات بين المستهلكين عن طريق الـرف الإلكـتروني Electronic Bay، حيـث يقـوم المسـتهلك بتقـديم البضـائع إلى المـزاد، ويستطيع المستهلكون الآخرون المزايدة على الـثمن، ويقـوم الـرف الإلكـتروني بالخدمـة كوسـيط حيث يتيح للعملاء وضع بضائعهم للبيع على الموقع

(1) د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، رسالة دكتوراه، كلية الحقوق، جامعة الإسكندرية، 2005، ص 46.

(2) د. رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص 32

الخاص بالرف الإلكتروني E-Bay، وهذا الشكل ينافس التجارة الإلكترونية التي تتم بين وحدة الأعمال والمستهلك.

6) **يرى جانب من الفقه الأمريكي أن هناك شكلا سادسًا للتجارة الإلكترونية البينية داخل المنظمة الواحدة Intra -Organizational - e-commerce ويشمل ذلك المنظمات العالمية التي تستخدم تكنولوجيا الإلكترونيات للاتصال بين فروعها أو أقسامها أو الشركات التابعة لها، مثال ذلك أن يتم برمجة جهاز كمبيوتر إحدى الشركات مسبقًا على أنه في حالة نقصان البضاعة الموجودة في الشركة عن مقدار معين ينشط البرنامج تلقائيًا ويرسل رسالة إلكترونية لجهاز الكمبيوتر الرئيسي الذي يقوم بتلقي الرسالة وإصدار أمر يظهر على الشاشة بإرسال البضائع المطلوبة، مع توجيه أمر آخر بعمل مقاصة حسابية إلكترونية بين فرع الشركة ومخزنها لسداد قيمة البضاعة المنصرفة.**(1)

ويمكننا القول بأن هذه الصورة لا تتعدى العملية التنظيمية في وحدة المنظمة التجارية أكثر من كونها شكلا من أشكال التجارة الإلكترونية.

المطلب الرابع

تقدير التجارة الإلكترونية

أولا: مزايا التجارة الإلكترونية:

تدل التقديرات المختلفة للمعاملات الإلكترونية والتجارة عبر شبكة الإنترنت أنها قد تزايدت خلال سنوات قليلة وأصبحت تقدر بالمليارات بعد أن كانت تقدر بملايين الدولارات، ولا ريب أن هذه الزيادة السريعة

(1) د. خالد ممدوح إبراهيم محمد، إبرام العقد الإلكتروني، مرجع سابق، ص 67.

والمطردة قد جاءت تعبيرًا صادقًا عما تحققه التجارة الإلكترونية من مزايا عديدة للمتعاملين بها بائعين أو مستهلكين، ولا شك في أن عالمية التجارة الإلكترونية قد فتحت الأبواب لإجراء المعاملات بصورة سريعة، ونظمت الجهود الدولية، واخترقت الحواجز وتجاوزت الحدود، فضلا عن تمكينها من استخدام وسائل إدارة النشاط التجاري سواء بأسلوب العرض أم بالطلب أم بالتسويق، ناهيك عن تلبية متطلبات الزبائن وتفهم احتياجاتهم، يضاف إلى ذلك أن التجارة الإلكترونية تساهم بشكل فعال في قياس الأداء وتطوير الخدمات وزيادة المعرفة، ويمكننا تلخيص هذه المزايا على النحو التالي.

1 - بالنسبة للبائعين:

- يتيح هذا النوع من التجارة للبائعين عرض سلعهم ومنتجاتهم وخدماتهم على عدد أكبر من جمهور المستهلكين والمشترين، بعد أن كان عرضهم لهذه المنتجات والسلع والخدمات مقصورًا على قاعدة أصغر من الجمهور، مثل المترددين على المتجر الفعلي ومن تصل إليهم إعلاناته ودعايته، وهم أقل من أعداد المترددين على المراكز التجارية الافتراضية من خلال شبكة الإنترنت، فانفتحت للبائعين بذلك أسواق جديدة، لم يكن متاحًا لهم الدخول فيها بهذه السهولة لولا شبكة الإنترنت والتجارة الإلكترونية.
- تعمل هذه التجارة على التقليل من النفقات التي كانت تنفق من قبل في التسويق التقليدي بالبلدان الأخرى، مثل الاشتراك في المعارض الخارجية، وإرسال البعثات الترويجية، والدعاية لها بأجهزة الإعلام المختلفة؛ إذ يمكن من خلال شبكة الإنترنت عرض جميع المنتجات والسلع والخدمات وما يصاحبها من معلومات مهمة متعلقة بالمواصفات المتوفرة للسلع والمنتجات والخدمات وسبل الحصول

عليها دون الحاجة إلى النفقات الكثيرة التي كانت تنفق في التسويق التقليدي.[1]

- تعمل هذه التجارة على توفير الجهد على جمهور البائعين في الانتقال إلى جمهور المشترين في أماكنهم المختلفة، إذ يمكن الوصول إلى الغاية ذاتها بمجرد إنشاء الموقع أو المجمع الافتراضي أو الفاترينة الافتراضية على شبكة الإنترنت، وتزويدها بكافة البيانات اللازمة للترويج للمعروضات.
- توفر على البائعين الوقت، إذ يمكن لكل منهم التعاقد وإبرام الصفقات مع أكثر من شخص من جمهور المشترين من بلدان مختلفة في الوقت ذاته دون حاجة إلى الانتقال لجمهور هذا البلد مرة، وجمهور البلد الآخر مرة أخرى، ودون حاجة إلى اتخاذ إجراءات كثيرة.
- زيادة روح التنافس بين البائعين بعرض أفضل ما لديهم في أحسن صورة لاختراق الأسواق والوصول إلى العملاء.

2- بالنسبة للمشترين:

- تتيح هذه التجارة للمشترين الفرصة في زيارة مراكز تجارية افتراضية أكثر للتعرف على ما بها من محلات، والوقوف على ما يقدمه كل منها من سلع وخدمات ومنتجات والمفاضلة بينها، واختيار الأنسب منها بأقل مجهود بل وهو في منزله أو في مكانه، وبأقل قدر من النفقات.
- الاستفادة من التنافس الحاصل بين العارضين في الحصول على أفضل

(1) Charles Chatterjee، Ecommerce law for Business Managers, Financial World publishing, London, 2002، p 200.

سلعة أو خدمة بأقل ثمن.[1]

ثانيا: عيوب التجارة الإلكترونية:

لا جدال في أن إدخال الحاسب الإلكتروني وشبكة الإنترنت في مجال التجارة قد أتى بالعديد من المزايا للمتعاملين في هذا المجال، وقد بينت الدراسة جانبًا منها سواء بالنسبة للمتعاملين من البائعين ومقدمي الخدمات، أو المتعاملين من المشترين ومتلقي الخدمات، إلا أنه لما كان لكل تطور وتقدم ضريبته ومخاطره فإن إدخال الحاسبات الإلكترونية في مجال التجارة يثير الخشية من المشكلات والعيوب والمخاطر التالية:

1 - مشكلة إثبات التصرفات:

يشكل الورق الدعامة المعتادة للمستندات العقدية التقليدية، ويتمتع بقيمة كبيرة في الإثبات في إطار ما يعرف بالدليل الكتابي، بينما تؤدي المعلوماتية عمومًا ومنها التجارة الإلكترونية إلى تجريد الكتابة من الطابع الورقي، فبرغم التطور الهائل الذي تشهده الكتابة أو المحررات الإلكترونية أو المعلوماتية لا يزال تبادل المستندات الورقية في وقتنا الحالي هو الأكثر أهمية، ويرجع ذلك إلى صعوبة الإثبات التي تثيرها المعلوماتية، ولا تزول هذه الصعوبة بالمصادقة الإلكترونية.[2]

2- مشكلة الاستخدام غير المشروع لبيانات الطرفين من جانب طرف ثالث:

أثار انتشار استخدام الحاسب الإلكتروني على نطاق واسع بين المشروعات والمؤسسات والأفراد مشكلات عديدة، منها قيام البعض بتتبع

(1) Charles Chatterjee، Ecommerce law for Business Managers, Financial World publishing، op، cit، p 202.

(2) د. إبراهيم أبو الهيجاء، القانون الواجب التطبيق على عقود التجارة الإلكترونية، رسالة دكتوراه، حقوق القاهرة، 2004، ص50.

البيانات الخاصة بالآخرين على شبكة الإنترنت بصورة غير قانونية، حتى إنه أصبح متاحًا لبعض الهواة والمحترفين النفاذ إلى مراكز المعلومات سواء الخاصة بالأفراد أو بالمراكز التجارية أو بمراكز المعلومات العسكرية لبعض الدول، حيث تمكن أحد الهواة في أوروبا من حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية)، وأصبح السبيل أمامه مفتوحًا للعبث ببيانات هذا المركز.

وفي هذا الإطار لم يعد صعبا التدخل بشكل غير مشروع في بيانات متجر أو مركز افتراضي من ناحية، أو استخدام كود الدخول لشبكة الإنترنت الخاص بشخص آخر في الحصول على خدمة متجر أو مركز افتراضي من سلع أو منتجات أو خدمات.

3- مشكلة الترويج لسلع أو خدمات محظورة:

فالتعامل التجاري عبر شبكة الإنترنت يتيح للبعض اللجوء إلى طرق غير مألوفة لترويج سلع أو منتجات أو خدمات محظورة في البلدان التي يقيمون على أرضها.[1]

4- مشكلة مدى حجية التوقيع الإلكتروني:

أثار ظهور التوقيع الإلكتروني تساؤلات حول مدى إمكانية اعتماده بالقدر ذاته الذي يعتمد به التوقيع التقليدي[2] الذي يضعه الشخص بخط يده على المحرر الكتابي الذي تتم تهيئته ليكون دليلا في الإثبات، فهناك جانب

(1) د. ميرفت عبد المنعم صادق، الحماية الجنائية للمستهلك، رسالة دكتوراه، حقوق القاهرة، 1999، ص 8.
(2) د. أحمد شرف الدين، الجوانب القانونية للتجارة الإلكترونية وآليات حل منازعاتها، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي 10: 12 مايو 2003.

كبير من الفقه رفض اعتبار التوقيع الإلكتروني مماثلا للتوقيع بخط اليد، وجانب آخر أيد اعتباره مماثلا للتوقيع بخط اليد، بل إن البعض ذهبت به الثقة في هذا التوقيع إلى حد القول بأن التوقيع الإلكتروني يتفوق على التوقيع التقليدي الذي يتم بخط اليد، بالنظر إلى أن التأكد من شخصية صاحب التوقيع يتم بشكل روتيني في كل مرة يتم فيها استخدام الرقم السري أو المفتاح الخاص، وبالتالي فإنه لا مجال للانتظار حتى ينشب النزاع للبحث في مدى صحة التوقيع كما هو الشأن في أغلب الأحوال بصدد المحررات الموقعة بخط اليد، ويعلل ذلك بأن الثقة في صحة التوقيع الإلكتروني من عدمها لا تتعلق بقواعد الإثبات بقدر ما تتعلق من ناحية بكفاءة التقنيات المستخدمة في تأمين مضمون المحرر المدون إلكترونيا[1]، وتأمين ارتباطه بشكل لا يقبل الانفصال عن التوقيع من ناحية أخرى، لذا فعلى القاضي قبل أن يقبل أو يرفض المحرر الموقع عليه إلكترونيًا أن يتأكد أولا من مدى كفاءة التقنية المستخدمة في استيفاء الشروط التي تؤهل التوقيع للقيام بدوره في الإثبات، ويؤخذ على هذا الرأي أنه يفرط في ثقته بالتوقيع الإلكتروني ويغفل عدة أمور مهمة منها:

1) أن الرقم السري أو المفتاح الخاص بالربط بين التوقيع والمحرر غير مأمون دائمًا مهما بلغت درجة التقنية المستخدمة، فبرغم التقنية العالية المستخدمة في مراكز المعلومات بالبنتاجون (وزارة الدفاع الأمريكية) تمكن أحد الهواة من فك شفرتها، وأصبح السبيل أمامه مفتوحًا للعبث

(1) د. إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي من 10: 12 مايو 2003، إدارة المطبوعات، جامعة الإمارات، المجلد الخامس، ص 1845.

ببيانات هذا المركز، الأمر الذي نستطيع معه القول بإمكانية قيام آخرين بفك شفرة الأرقام السرية والمفاتيح الخاصة بالربط بين التوقيع والمحرر.[1]

2) من دلائل عدم الأمان التي تحيط بالرقم السري أو المفتاح الخاص بالربط بين التوقيع والمحرر أنه ينبغي أن يقوم الموقع بإجراء هذا التوقيع في سرية تامة بعيدًا عن أي من المحيطين به، إذ لو تمكن أي منهم من التعرف على الرقم السري أو المفتاح الخاص بالربط بين المحرر والتوقيع خلسة أو مصادفة، فسيتمكن من خلاله من إجراء معاملات وإجراء صفقات لحسابه.

3) أن من شأن القول بأن على القاضي أن يقرر مدى كفاءة التقنية المستخدمة في استيفاء الشروط التي تؤهل التوقيع للقيام بدوره في الإثبات إلقاء عبء جديد على القضاء ونقل عبء الإثبات إليه، وهو أمر غير مستساغ.

يضاف إلى ذلك مشكلات أخرى في الوفاء، والملكية الفكرية، والقانون الواجب التطبيق، والجانب الضريبي، وغيره من الجوانب الاقتصادية والاجتماعية والأخلاقية والثقافية مما لا يتسع المقام للوقوف عليها جميعًا، ويحتاج كل جانب من هذه الجوانب المتعددة إلى دراسة متخصصة.[2]

ومن المشكلات الأخرى التي تثار في هذا الصدد مشكلة عدم وجود طرف ثالث بين البائع من ناحية وبين المشتري، بحيث يضمن للأول شحن السلعة أو المنتج ولا يوافي الطرف الآخر بالخدمة إلا بعد أن يحصل على

(1) Christiana Feral،Schuhl، Cyber Droit le droit 'a l'epreuve de l'internet- OP، CIT، p 203.
(2) د. حسام الدين الأهواني، حماية حقوق الملكية الفكرية، مرجع سابق، ص 26.

قيمتها، ويضمن للمشتري ألا يدفع هذه القيمة إلا بعد التأكد من أن السلعة أو الخدمة في سبيلها للوصول إليه على النحو المتفق عليه في التعاقد المبرم بينهما.

بالإضافة إلى عدم الثقة بين المتعاملين بالتجارة لعدم وقوفهم على يقين من الأطراف بالحصول على السلعة أو الخدمة المطلوبة، وإشكاليات التكلفة المالية الإضافية والتي تتمثل في تكلفة المعرفة أو الاستشارة القانونية، ولا شك في أن صيانة وكلفة تطوير أنظمة التجارة الإلكترونية تتطلب وجود مخصصات مالية كافية.

كما أن العديد من الدول لم تقر قوانين خاصة بالتجارة الإلكترونية، الأمر الذي يؤدي إلى الإحجام عن التعامل مع أية دولة لم تضع التشريعات الكافية والكفيلة بحماية مصالح المتعاقدين، أو أن التشريعات الموجودة في بعض الدول لا تكون كافية لتحقيق متطلبات التجارة الإلكترونية ورغبة الطامحين إليها، كما تواجه التجارة الإلكترونية تحديات عظمى تتمثل في الفيروسات والاختراقات والتي تؤثر سلبا على هذه التجارة وتطورها.



المبحث الثاني

خصائـص التجارة الإلكترونية ومعـوقاتها ومستقبلها

تعرف التجارة الإلكترونيـة بأنهـا العمليـات التجاريـة التـي تـتم عـبر المبـادلات الإلكترونيـة، وتعرف المبادلات الإلكترونية بأنها تلك التـي تـتم باسـتعمال الوسـائط الإلكترونيـة[1] دون وجـود علاقة مباشرة بين طرفي العقد، ودون الاعتماد على الوسائط الورقية، وكـل ذلـك يـؤدي إلى اتسـاع مجال العلاقات التجارية في التجارة الإلكترونية.

وعلى الرغم مما تتيحه التجارة الإلكترونية من فـرص إيجابيـة للاقتصـاد الـوطني وللاقتصـاد العالمي، إلا أن هناك عوامل إضافية لا تزال تعيق حركة التجارة الإلكترونية وتطورها.

وفي مواجهة هذه الصعوبات فإنه من الضروري اتبـاع إسـتراتيجيات خادمـة لقطـاع التجـارة الإلكترونية في كافة المجالات القانونية والمصرفية والتأمينية والضريبية، كون التجارة الإلكترونية في حقيقتها وجوهرها عملا تجاريـا، ومـن خصائصـها تـلاشي الكتابـة لانسـياب البيانـات مـن شـبكة الإنترنت، وهي تستند إلى فكرة العولمة، لذا فإن متطلباتها تتمثـل في تطـوير التجـارة الإلكترونيـة وتشجيعها، وتوفير خدمات الاتصالات الموثوقة، وتـوفير بيئـة قانونيـة داعمـة، وأنشـطة تثقيفيـة للبناء الذاتي للتجارة الإلكترونية، بالإضافة إلى دور القطاع العام في تطبيـق تكنولوجيـا المعلومـات في الإدارة العامة للدولة لزيادة شـفافية إجراءاتهـا، إضـافة إلى تبسـيط الإجـراءات، ورفـع كفـاءة وجودة تكنولوجيا المعلومات.

(1) المادة الثانية من قانون التجارة والمبادلات الإلكترونية التونسي- قـانون رقـم 83 لسـنة 2000 الصـادر في 9 أغسطس 2000.

وسوف نتناول هذا المبحث وفق المطالب التالية:

المطلب الأول: خصائص التجارة الإلكترونية

المطلب الثاني: معوقات التجارة الإلكترونية

المطلب الثالث: مستقبل التجارة الإلكترونية

المطلب الأول

خصائص التجارة الإلكترونية

تعتمد التجارة الإلكترونية على تقنية حديثة ومتطورة، تسمح بإبرام العقود الخاصة بتجارة السلع والخدمات بين وحدات الأعمال بعضها البعض (B TO B) وبين وحدات الأعمال والمستهلك (B TO C) وبين وحدات الأعمال والإدارة الحكومية ويرمز لها (B to A) عن بعد دون الحاجة لانتقال الطرفين أو لقائهما، كما أن هذه التجارة تتم باستخدام التبادل الإلكتروني للمستندات، والتحويلات الإلكترونية للأموال، وسوف نتناول في هذا المطلب خصائص التجارة الإلكترونية والتي يمكن إجمالها فيما يلي:

أولا: عدم وجود علاقة مباشرة بين طرفي العقد:

السمة الرئيسية التي تهيمن على هذه التجارة الإلكترونية اعتمادها على تقنية حديثة ومتطورة لتذليل أي عقبات مادية أو قانونية في المعاملات الدولية والمحلية.

ففي عقود التجارة الإلكترونية لا يكون هناك مجلس للعقد بالمعنى التقليدي، فمجلس العقد الإلكتروني مجلس افتراضي، فقد يكون البائع في مكان والمشتري يبعد عنه آلاف الأميال، وقد يختلف التوقيت الزمني أيضًا بين مكاني البائع والمشتري اعتمادًا على علاقة تقنية حديثة ومتطورة يتم من خلالها التلاقي بين طرفي المعاملات التجارية من خلال شبكة الاتصال،

وبالرغم من أن هذا النموذج ليس جديدًا حيث شهدت التجارة الاستخدام المكثف لوسائل الاتصال الحديثة مثل الفاكس، إلا أن ما يميز هذا الأسلوب هو وجود درجة عالية من التفاعلية بغض النظر عن وجود طرفي التفاعل في الوقت نفسه على الشبكة وهو ما دفع البعض إلى القول بأن للتجارة الإلكترونية تأثيرًا سلبيًا على العلاقات الاجتماعية بين الأفراد نتيجة غياب العلاقات الحميمة بين المتعاقدين.[1]

ونتيجة لغياب هذه العلاقات المباشرة بين الأطراف المتعاقدة كان هناك وسيط إلكتروني بين طرفي التعاقد، وهو جهاز الكمبيوتر أو البرنامج المتصل بشبكة الاتصالات الدولية التي تقوم بنقل التعبير عن الإرادة إلكترونية لكل من الطرفين المتعاقدين في اللحظة ذاتها رغم انفصالهما مكانيا.

وهنا يمكن أن يثور التساؤل عن مدى مسئولية مقدم خدمة شبكة الإنترنت عن عدم وصول الرسالة أو وصولها متأخرة عن الميعاد، أو تحريفها أو وجود غلط بها.

عالج المشرع المصري حالة تدخل أحد القائمين بأعمال الاتصالات تدخلا إراديًا في التلاعب في الرسائل بتوقيع عقوبة جنائية، إذ نص القانون رقم 10 لسنة 2003 بشأن تنظيم الاتصالات[2] في المادة 73 منه على أنه: "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام

(1) د. سمير برهان، إبرام العقد في التجارة الإلكترونية بحث مقدم إلى مؤتمر الجوانب القانونية للتجارة الإلكترونية، والمنعقد بالقاهرة في الفترة 12، 13 يناير 2002.

(2) صدر هذا القانون في 4 فبراير 2003 ونشر بالجريدة الرسمية في العدد رقم 5 مكرر (أ) في 4/ 2/ 2003.

أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية... إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو جزء منها تكون قد وصلت إليه".

إلا أنه في القانون الإماراتي لا نجد نصًا مماثلا لهذا النص، وإنما نص المشرع في القانون الاتحادي رقم (3) لسنة 2003 في شأن تنظيم قطاع الاتصالات[1] في المادة (72) على معاقبة كل من استغل أجهزة أو خدمات الاتصالات في الإساءة أو الإزعاج أو إيذاء مشاعر الآخرين أو لغرض آخر غير مشروع، كما عاقب كل من نسخ أو أفشى أو وزع بدون وجه حق فحوى أي اتصال أو رسالة هاتفية مرسلة من خلال استخدام شبكة اتصالات عامة، ونص كذلك على معاقبة كل من يتنصت على محتوى المكالمات أو مضمونها دون إذن مسبق من السلطات القضائية المختصة.

كما جاء نص القانون الاتحادي رقم 2 لسنة 2006 بشأن المعاملات والتجارة الإلكترونية في مادته الثانية على النحو التالي:

1) " كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي، سواء بدخول الموقع أو النظام أو بتجاوز مدخل مصرح به يعاقب بالحبس وبالغرامة أو بإحدى هاتين العقوبتين.

2) فإذا ترتب على الفعل إلغاء أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين.

ونص في مادته الثالثة على أن كل من ارتكب أيًا من الجرائم المنصوص عليها في البند (2) من المادة (2) من هذا القانون أثناء أو بسبب تأدية عمله أو سهل ذلك للغير يعاقب بالحبس مدة لا تقل عن سنة والغرامة

(1) صدر هذا القانون بمرسوم بتاريخ 15/ 11/ 2003.

التي لا تقل عن عشرين ألف درهم أو بإحدى هاتين العقوبتين.

من ناحية أخرى ونتيجة لعدم وجود علاقة مباشرة بين الأطراف المتعاقدة، وعدم إمكانية تحديد هوية المتعاقدين، وذلك نتيجة للانفصال المكاني بين أطراف المعاملات التجارية الإلكترونية، وعدم معرفة كافة المعلومات الأساسية عن بعضهم البعض كما هو الحال في المعاملات التجارية التقليدية، فقد لا يعرف أي منهما درجة يسار الآخر أو مركزه المالي، وهل بلغ سن الرشد أم أنه ناقص الأهلية.

ثانيا: عدم الاعتماد على الوثائق الورقية:

من أهم الخصائص التي تميز التجارة الإلكترونية هي أن كافة المعاملات والعمليات التي تتم بين طرفي المعاملة تتم إلكترونيا دون استخدام أي ورق في إجراء وتنفيذ المعاملات، وبالتالي تصبح الرسالة الإلكترونية هي السند القانوني الوحيد المتاح لكلا الطرفين في حالة نشوب أي نزاع بينهما[1].

ولذلك فإن الهدف من التجارة الإلكترونية هو خلق مجتمع المعاملات اللاورقية، وإحلال دعائم إلكترونية محل الدعائم الورقية، وهو ما يعني الاستغناء عن التعامل بالمستندات الورقية ليحل محلها المستند الإلكتروني[2]، وذلك بعد أن تكشفت بعض سلبيات العمل بتلك المستندات

(1) رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص13.

(2) د. السيد عتيق، جرائم الإنترنت، دار النهضة العربية، القاهرة، 2000 ص120.

والمستند معناه وفقا لقانون التوقيع الإلكتروني المصري 2004/15 " أن يكون للمحرر ولو في الظاهر مرسل يحتج بصدور المحرر منه، بالتالي لا يعد محرر ما مستندا إذا كان غير ظاهر من هو المرسل الذي انبعث منه هذا المحرر". وعرف المحرر الإلكتروني بأنه رسالة بيانات تتضمن معلومات تنشأ أو تدمج أو تخزن أو ترسل أو تستقبل كليا أو جزئيا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية =

من بطء حركة الإرسال والاستقبال، وقابلية محفوظات المستندات الورقية للتضخم وشغلها مزيدا من غرف الحفظ، واحتياجها العاملين للقيام بهذا العمل، بالإضافة إلى صعوبة التداول، خاصة في ظل ثورة الاتصالات والمعلومات التي يشهدها عالمنا المعاصر.[1]

= وسيلة أخرى مشابهة".

(1) تعد تجربة شركة إنتل من التجارب الرائعة في هذا المجال, حيث إنها من كبريات الشركات المنتجة والمصدرة للشرائح والمعالجات، وتبيع منتجاتها إلى كبرى شركات تصنيع التقنية، وغالبية المبيعات تدخل في صناعة الحواسب الآلية حيث بعض الشركات المصنعة للحواسب الآلية مثل Dell تستخدم فقط معالجات إنتل، وبعض الشركات المصنعة للحواسب الآلية تستخدم معالجات إنتل ومعالجات منافسيها أيضا، والمنافسة شديدة جدا في عالم الشرائح، فتصمم إنتل كاتالوجات شخصية وترسلها إلى الزبائن من أجل إتمام صفقات تجارية، وإلى عام 1998 فإن هذه العملية كانت تتم من خلال الورق، مما يجعل عملية التوزيع بطيئة ومكلفة وفي كثير من الأوقات تصبح هذه الكاتالوجات قديمة ولا تحتوي على المعلومات الجديدة والحديثة.

بعض الشركات الكبرى من مثل سيسكو وديل بدأت باستخدام شبكة الإنترنت بشكل صغير في 1995 و1996، وتوسعوا ولكن بعجلة بطيئة. وفي المقابل لم تهرول إنتل في اتجاه التجارة الإلكترونية، وعندما افتتحت إنتل في صيف 1998 موقعها الإلكتروني للبيع على شبكة الإنترنت أرسلت تقارير تذكر فيها أن حجم مبيعاتها من خلال التجارة الإلكترونية زادت من صفر إلى بليون دولار خلال شهر واحد فقط، ونرى أن سيسكو احتاجت 6 أشهر لكي تصل لهذا المقدار!!! لماذا؟؟

التجارة الإلكترونية في 1998 كانت أكثر تقدمًا وتحضرًا من عامي 1995 أو 1996، كما أن إنتل بنت نظامًا أكثر شمولية، استثمرت إنتل التجارة الإلكترونية كطريقة جديدة من أجل الاتجار، ولذلك فإن إدارة الشركة قررت أن تجعل التجارة الإلكترونية حدثًا مهمًا في تاريخ الشركة لكي يشعر الزبون بجدية الشركة حول التجارة الإلكترونية.

الموقع هو عبارة عن شبكة خارجية تسمى ببرنامج التجارة الإلكترونية=

ثالثًا: اتساع مجال العلاقات التجارية في التجارة الإلكترونية:

تتضمن التجارة الإلكترونية التلاقي الجماعي بين عدة أطراف بحيث يمكن لأحد أطراف المعاملة إرسال رسالة إلكترونية إلى عدد لا نهائي من المستقبلين في الوقت نفسه ودون حاجة لإعادة إرسالها كل مرة، وفي هذا توفر شبكة الإنترنت إمكانيات بلا حدود للتفاعل الجماعي بين الأفراد، وهو شيء غير مسبوق في أي أداة تفاعلية سابقة.

فقد تكون الرسالة موجهة إلى أشخاص غير معينين، إذ يستطيع المرسل إرسال الرسالة الإلكترونية عبر البريد الإلكتروني إلى عشرات الأشخاص في وقت واحد وفي عدة دول، أي أن العلاقات القانونية الناشئة عن هذه

= Business Program،E ويركز هذا البرنامج على توفير الدعم الفني للعديد من المنتجات من مثل المعالجات واللوحات الأم والذاكرات الوماضة، وفي عام 1998 استطاعت إنتل أن تصل إلى المئات من الشركات متوسطة وصغيرة الحجم حول العالم، وهذه الشركات قامت بإرسال طلبياتها عبر المتصفحات، فالدخول إلى هذا الموقع مسموح فقط للشركاء التجاريين المخول لهم بالدخول.
وإرسال الطلبيات هو جزء فقط مما توفره إنتل لزبائنها، فالموقع أيضا يوفر خدمة تتبع الطلبيات، ومكتبة إلكترونية تحتوي على الكثير من الوثائق الخاصة بالمنتج، وكل هذه الأعمال تقلل من الضغط على مسئولي خدمة الزبائن الذين كانوا يرسلون هذه المعلومات بصورة يدوية مسبقا.
وفي هذا التطور الجديد لإنتل فإن الشركة اتجهت لتعميم البرنامج على الشركات الصغيرة ومتوسطة الحجم التي كانت مجمل اتصالاتها بإنتل عن طريق التليفون والفاكس، في حين أن اتصالات شركة إنتل مع الشركات الكبيرة كانت تجري عبر شبكات التبادل الإلكتروني للبيانات electronic data interchange أو EDI.
فما هي نتائج هذا التحول؟ مسئولو شركة إنتل يقولون بأن الشركة وفرت 45.000 فاكس في كل ثلاثة أشهر إلى تايوان لوحدها، وذلك في عام 1999. http://www.arabcin.net.

التجارة ليست حبيسة مكان معين ودولة معينة، ولكنها تنساب عبر الدول في حرية تامة ترفض الخضوع لأي سيطرة سياسية أو التقيد بحدود جغرافية معينة[1].

ونتيجة لاتساع مجال التجارة الإلكترونية وسرعة إنجاز الصفقات التجارية يتضح أن التجارة الإلكترونية تساهم بشكل فعال في إتمام العمليات التجارية بين الأطراف على وجه السرعة ابتداءً من مرحلة التفاوض وإبرام العقود، وحتى الدفع الإلكتروني والانتهاء بتسليم المنتجات ماديًّا بإحدى الطرق التقليدية من شحن أو عن طريق البريد، أما الخدمات الإلكترونية فيتم تسليمها إلكترونيًّا مثل برامج الحاسب الآلي، التسجيلات الموسيقية، أفلام الفيديو، الكتب والأبحاث والتقارير الإلكترونية، إلى جانب بعض الخدمات مثل الاستشارات الطبية أو الهندسية أو القانونية، وهو ما قد يخلق نوعًا من التحدي للسلطات المختصة حيث إنه لا يوجد حتى الآن آليات متفق عليها لإخضاع المنتجات الرقمية للجمارك أو الضرائب، فقد يستغل البائعون ذلك للتهرب من سداد الجمارك والضرائب بعدم تسجيل هذه التعاملات في الدفاتر المحاسبية الرسمية.

ويتبين لنا من خلال عرضنا لخصائص التجارة الإلكترونية أن العقد الإلكتروني سوف يبرم على دعامة إلكترونية وذلك لاختفاء الدعامة الورقية، كما أن التعاقد الإلكتروني يتم من خلال شبكة اتصالات دولية، ويتم تسليم المنتجات ماديًّا والخدمات إلكترونيًّا على الخط online.

(1) د. محمد السيد عرفة، التجارة الدولية الإلكترونية عبر شبكة الإنترنت ومفهومها والقاعدة القانونية التي تحكمها ومدى حجية المخرجات في الإثبات، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة، الفترة من 1: 3 مايو 2000، ص1.

ويصعب تحديد هوية المتعاقدين مما يخلق اتساعًا للمجال التجاري للتجارة الإلكترونية مع إمكانية التعامل الجماعي بين عدة أطراف متعاقدة من خلال شبكة الإنترنت.[1]

المطلب الثاني

معوقات التجارة الإلكترونية

تتمثل أبرز عوائق التجارة الإلكترونية في الجوانب الأمنية، التي من بينها إمكانية قيام قراصنة الكمبيوتر باختراق مواقع التجارة الإلكترونية في بعض الأحوال وسرقة المعلومات الموجودة بها، والتي قد يكون من بينها أرقام بطاقات العملاء، كذلك يمكن تخريب هذه المواقع أو تدميرها عن طريق الفيروسات، أو تغيير محتوياتها، أو تعطيلها عن العمل، أو محو البيانات الموجودة بها.

وتتعدد المخاطر التي تتعرض لها شبكة الإنترنت في تداول البيانات، الأمر الذي يؤثر سلبًا على التجارة الإلكترونية، ويؤدي إلى وجود نوع من التردد في استخدام شبكة الانترنت, وقد تم تصنيف مستخدمي الشبكة بحسب أسباب إحجامهم عن التعامل بالتجارة الإلكترونية إلى الأصناف الآتية:

- 53% من أسباب تردد العملاء في استخدام الشبكة يرجع إلى عدم وجود الأمان security الكافي بالنسبة للعميل.
- ويأتي في المرتبة التالية صعوبة التجول والاتصال والتعامل بنسبة 35%.
- ثم عدم التعامل لعدم وجود اختيارات كافية بنسبة 27%.

(1) د. نافذ ياسين محمد المدهون، النظام القانوني للتجارة الإلكترونية، مرجع سابق، ص 117.

- ثم لعامل عدم الثقة بنسبة 24%.
- ثم لارتفاع الأسعار بنسبة 20%.

كما أن هناك بعض المشكلات الأخرى التي تتمثل في إمكانية تعطيل مواقع التجارة الإلكترونية، ومن أهم المخاطر التي يمكن أن يتعرض لها أي مشروع مشترك في التجارة إلكترونية ما يلي:

أ - الكشف عن الأسرار:

وذلك إذا كانت الصفقات التجارية تتضمن في الغالب نصًا يوجب على الأطراف الالتزام بالسرية وعدم الإفشاء، فإنه من المحتمل أن يهدد مثل هذا الاتفاق خاصية انفتاح شبكة المعلومات العالمية[1] أمام جميع مستخدميها؛ إذ من المحتمل الكشف لمنافسين أو لأناس آخرين عن معلومات خاصة بالتسويق أو بالممتلكات مثل حقوق الملكية الفكرية أو بالأسعار المنافسة والتي تكون حاسمة في نجاح الأعمال.

ب - خسائر مالية مباشرة:

قد تتعرض مواقع التجارة الإلكترونية للاحتيال في بعض الأحيان كنقل أموال من حساب إلى آخر بدون وجه حق، أو تدمير أو إخفاء سجلات مالية قد تكشف عن تصرفات غير قانونية، فالمشترون (على سبيل المثال) يخشون من إرسال معلومات عن بطاقاتهم الائتمانية على الشبكة، بينما تزداد الحاجة إلى الأمن مع تحرك العمل نحو التجارة الإلكترونية القائمة على الصفقات، وحتى مواقع التسويق غير منيعة أمام الأضرار والخسائر الناجمة عن انتهاك الأمن وخرقه.[2]

---

(1) د. حسن الماحي، نظرات قانونية في التجارة الإلكترونية، مرجع سابق، ص 186.

(2) Efraim Turban & Jae Lee & David King & H.Michael Chung، Electronic Commerce A Managerial Perspective، Prentice Hall، Inc، New Jersey، 2000 P 395

ومن أحدث التطبيقات القضائية في هذا المجال بولاية كاليفورنيا في الولايات المتحدة الأمريكية، أنه تم القبض على شخص قام بالاستيلاء على أرقام بطاقات الائتمان، وتم الحكم عليه بالحبس لمدة عشرة شهور في 3 مارس 2008[1]، وفي قضية أخرى وتحديدًا في 26 فبراير 2008 حكم على شخص بالحبس لمدة خمسين شهرًا لقيامه بسرقة حوالي 637.000 كارت ائتمان، وتم استخدام هذه الكروت في عمليات من خلال مواقع شبكة الإنترنت.[2]

ج - تكاليف غير متوقعة:

كثيرًا ما يتعرض المتعامل عبر الشبكة لتحمل تكاليف قانونية لم تكن في حسبانه بسبب اختراقات خارجية، أو عدم أمانة أحد العاملين، أو عدم وجود سيطرة ورقابة كافيتين، أو إخفاق في النظام الإلكتروني، بما يترتب عليه تأخر في إنهاء المعاملات، الأمر الذي من شأنه نشوب خلافات بين أطراف التعاقد وتحمل تكاليف غير متوقعة.

د - فقدان الثقة في التعامل عبر شبكة الإنترنت:

كثرة المشكلات والجرائم التي قد تنشأ عن استخدام شبكة الإنترنت وإحجام البعض عن استخدامها، قد تؤدي إلى فقدان الفرص بالنسبة للأعمال، وعدم تحقيق الفوائد، فكثيرًا ما يتعرض المستهلكون لمخاطر بالرغم من قوانين حماية المستهلك، فالمستهلك الذي يعهد بأمواله إلى أنظمة

(1) Indonesian Sentenced To 10 Months In Prison For Hacking Into Hotel Business Kiosks And Stealing Credit Card Data
At: Http://Www.Cybercrime.Gov/Tandiwidjojosent.Pdf

(2) David U. Haltinner Sentenced To 50 Months Of Imprisonment For Selling Approximately 637,000 Stolen Credit Card Numbers.
at: http://www.cybercrime.gov/haltinnerSent.pdf

إلكترونية تتعرض لهجوم أو فشل من الممكن بلا شك أن يتكبد خسائر.[1]

والتجارة الإلكترونية تشترك في أشياء كثيرة مع مثيلتها التقليدية؛ لأن كلا منهما يتضمن أطرافًا تلتقي معًا لشراء أو بيع سلع أو خدمات، ويحتويان على دفع وتسليم حيث تتجه نية هؤلاء الأطراف في الحالتين نحو خلق اتفاق قابل للتنفيذ، ويبرر هذا التشابه الوظيفي الاتجاه السائد للتعديلات التدريجية على المبادئ التقليدية لكي تستوعب جوانب كثيرة للتجارة الإلكترونية، ورغم هذا التشابه إلا أن هناك اختلافات مهمة بينهما؛ فعلى سبيل المثال تقلل التجارة الإلكترونية من اشتراطات الاعتماد على السجلات الورقية لتوثيق أي تعامل من التعاملات، كما أنها تحد أيضًا من المشاركة البشرية.

عوائق التجارة الإلكترونية في الوطن العربي:

التجارة الإلكترونية في الوطن العربي تسير بخطوات بطيئة وذلك لعدة أسباب، ونتناول هذه الأسباب مع الأخذ بجمهورية مصر العربية كنموذج لهذه الدول العربية.[2]

---

(1) د. طاهر شوقي مؤمن، عقد البيع الإلكتروني، دار النهضة العربية، القاهرة، 2007، ص 17.

(2) أضافت إحدى الدراسات أن هناك مشكلات أخرى بجانب المشكلات التقليدية التي تعوق التجارة الإلكترونية في العالم العربي، مثل المخاطر التي تتعرض لها الشركات صاحبة المواقع على شبكة الإنترنت من تخريب بيانات وتشويش وتحويل واستبدال بيانات، وإساءة التعامل معها، علاوة على المخاطر التي يتعرض لها الأفراد عند التعامل مع الشركات, وأشارت إلى أنه من بين هذه المخاطر إفشاء المعلومات الخاصة بالعميل، والتعرض لعمليات النصب والاحتيال خاصة السطو على المعلومات المتعلقة ببطاقات الائتمان، وأوضحت هذه الدراسة أن عدد مستخدمي شبكة الإنترنت في مصر لا يزيد على 0.7 بالمائة من سكان مصر =

فقد بدأت ثورة شبكة الإنترنت في مصر عام 1993، ولم تبدأ التجارة الإلكترونية إلا بعد ذلك بكثير، واقتصر الأمر على ندوات وورش عمل حول الموضوع، ولكن لم تحدث ممارسة حقيقية، وفي هذا السياق حدثت محاولات من جماعات تهتم بنشر خدمة شبكة الإنترنت لتوجيه الاهتمام المصري رسميًا وشعبيًا إلى أهمية وضرورة الدخول في مجال التجارة الإلكترونية، وأنشأت جماعة شبكة الإنترنت لجنة بخصوص التجارة الإلكترونية استهدفت إيجاد حلقة وصل بين الشركات الرئيسية في مجال التجارة الإلكترونية وبين شركات القطاعين العام والخاص، وأصدرت مسودة تعتبر حجر الأساس لمبادرة التجارة الإلكترونية في مصر، وقد ظهرت عشرة مواقع عام 1998 لتقديم بعض التعاملات التجارية من خلال شبكة الإنترنت، ووصل عدد المواقع إلى 184 عام 2000، إلا أن عدد المواقع التي تبيع جيدًا يتراوح بين10ـ20 موقعًا.

وبالرغم من أن مصر حالها كحال أغلب الدول العربية، والتي بدأت في استخدام شبكة الإنترنت منذ بداية التسعينيات، إلا أن هناك عقبات تحول

= تتركز 82 بالمائة من هذه النسبة في القاهرة والإسكندرية، كما أنها تأتي في المرتبة الثانية بعد السعودية في اقتناء أجهزة الكمبيوتر، وذكرت أن البنية الاتصالاتية في بعض الدول العربية مازالت ضعيفة جدا مشيرة إلى أن متوسط عدد الخطوط الرئيسية للتليفونات لكل مائة نسمة لم يزد على 1.24 في السودان، و1.4 في جيبوتي، و0.72 في موريتانيا، منوهة بأن النسبة الكبرى من التجارة الإلكترونية تتركز في الدول المتقدمة حيث مستوى التعليم المرتفع والقدرة الشرائية العالية للفرد، وأشارت إلى أن عدد مستخدمي شبكة الإنترنت في مصر لا يزيد على 33 لكل مليون نسمة، فيما لم يزد عدد الحاسبات الشخصية على 1.9 بالمائة فقط من السكان، وتراوحت نسبة من يمتلكون خطوط تليفونات ما بين 8.6 بالمائة و10.4 بالمائة online.com/technology/?id=22726،east،http://www.middle

دون انطلاق التجارة الإلكترونية فيها ومنها ما يلي:

1 - العقبات القانونية

باستثناء دول عربية قليلة سبق ذكرها منها دولة الإمارات العربية المتحدة، والجمهورية التونسية، ودولة البحرين، والمملكة الأردنية الهاشمية، أصدرت قوانين منظمة للتجارة الإلكترونية، وتظل باقي الدول في الوطن العربي خالية من هذه التشريعات المهمة لهذا القطاع.[1]

(1) كشفت هيئة تنظيم الاتصالات في دولة الإمارات العربية المتحدة أنها قامت بوضع حزمة من الآليات والإجراءات التي تمكنها من تسهيل خدمات التجارة الإلكترونية عبر شبكة الإنترنت، وتأمين ممارسة هذه التجارة، في الوقت الذي قال فيه عدد من الخبراء الاقتصاديين والمصرفيين: إن التجارة الإلكترونية ستشهد انتعاشًا بالرغم من الأزمة المالية العالمية باعتبارها الأقل كلفة والأسرع والأكثر كفاءة.
وقد بدأت الهيئة في منح تراخيص لمزودي خدمات التصديق الإلكتروني، وهم المعنيون بتزويد مواقع التجارة الإلكترونية بالتقنيات الأمنية وشهادات المصادقة الإلكترونية، وذلك بهدف زيادة نسب الأمان في التجارة الإلكترونية ومكافحة عمليات النصب والتزوير في هذه التجارة, كما بدأت مبادرة بالتعاون مع حكومة دبي الإلكترونية بهدف تعزيز ثقة المستهلك بالمعاملات والمراسلات الإلكترونية.
وفي دراسة أجرتها مجموعات بحثية مؤخرًا، كشفت أن مدى انتشار مستخدمي التجارة الإلكترونية في الإمارات كان الأعلى عربيا حيث بلغ بنسبة 25.1 % من إجمالي عدد السكان، في حين كانت النسبة 14.3% في السعودية، و10.7 % في الكويت، فيما انخفضت نسبة الأفراد المستخدمين للتجارة الإلكترونية في لبنان إلى 1.6% من عدد السكان، وفي استبيان الحكومة الإلكترونية لسنة 2008 الذي أجرته للأمم المتحدة، فإن الإمارات حصلت على الترتيب الخامس بالنسبة للتعاملات الإلكترونية من ضمن 192 دولة من أعضاء الأمم المتحدة، وأيضًا حصلت على المرتبة 32 في الجهوزية الإلكترونية مما يجعلها الأولى عربيا، وقد حصلت أيضًا على المرتبة الـ 12 في المقاييس الأمنية للشبكة طبقًا لاستبيان الأمم المتحدة .
http://www.emaratalyoum.com/Articles/2008/11/Pages/11272008_6fe1a8d51e3244c7bac8afd11c4815c0.aspx

ففي مصر جاء قانون التوقيع الإلكتروني رقم 15 لسنة 2004 خاليًا من أي تنظيم للمعاملات والعقود الإلكترونية[1].

ومازال مشروع قانون التجارة الإلكترونية لم ير النور بعد، والذي عرف في مادته الأولى الخاصة بالتعريفات التجارة الإلكترونية بأنها " معاملة تجارية تتم عن طريق وسيط إلكتروني" ويلاحظ أن التعريف لم يحدد وسائل التجارة الإلكترونية، وبالتالي لم يحصرها في شبكة الإنترنت، وهو أمر جيد نظرًا للتطور التقني السريع الذي يمكن أن يتجاوز يومًا شبكة الإنترنت [2].

وفي النهاية فإن هناك ضرورة لإصدار التشريعات المتخصصة لتنظيم عمل التجارة الإلكترونية، إضافة إلى تدريب عدد من القضاة والمحامين للتعامل مع الكثير من القضايا التي ينطوي عليها هذا المجال المستحدث.

بالإضافة لما سبق فإن التجارة الإلكترونية خلقت تحديات لم تكن معروفة من قبل في ظل التجارة التقليدية، كما أنشأت مفاهيم مستحدثة تتطلب توحيد جهود الباحثين في مختلف التخصصات (القانونية والاقتصادية والمحاسبية والاجتماعية والسياسية)، وطرحت العديد من الأسئلة[3] التي أدت إلى ظهور اجتهادات بين رجال القانون، نوجز من هذه الأسئلة ما يلي:

(1) صدر القانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، ونشر في الجريدة الرسمية في العدد رقم 17 تابع (د) في 22 أبريل 2004.

(2) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص17.

(3) فتحي محمد عبد الغني، مقدمة إلى التجارة الإلكترونية وتطوراتها، ورقة عمل مقدمة للندوة الأولى حول التجارة الإلكترونية (نماذج اليونسترال)، الإسكندرية 9: 12 أبريل 2006، ص 17.

1) ما هي قواعد التعاقد الإلكتروني؟

2) ما هي المحكمة المختصة إذا حدث نزاع بين مشترين وسماسرة وبائعين من ولايات قضائية مختلفة؟

3) ما هو الموقف من العمليات التي تتم عبر التجارة الإلكترونية وتكون مشروعة في دولة أحد الأطراف ومجرمة في دولة الطرف أو الأطراف الآخرين (المقامرة والمراهنات) والدعارة والإباحية واستخدام الأطفال؟

4) كيف يمكن تحديد المسئول عن حالات الغش والتدليس والسرقة والاستخدام غير المشروع للبيانات والمعلومات حال حدوثها؟ وكيف يمكن إثباتها؟

5) لو اختلف تاريخ توقيع العقد الواحد بين طرفين في دولتين (أمريكا واليابان مثلا) فأي التاريخين يكون تاريخًا للتعاقد؟

6) كيف يمكن تحصيل الضرائب المستحقة عن أعمال المقامرة والمراهنات في حالة مشروعيتها قانونًا في إحدى دول المتعاملين؟

7) ما هي الدولة التي يكون لها الحق في تحصيل الضرائب المستحقة على معاملات التجارة الإلكترونية (دولة البائع أم دولة المشتري أم الدولة التي فيها موقع الشركة؟

8) كيف يمكن حماية الأخلاق والتقاليد الوطنية والنظام العام والآداب العامة؟

9) كيف يمكن مواجهة عمليات غسل الأموال التي تستخدم فيها البطاقات الذكية بمبالغ ضئيلة؟

2 - العقبات التقنية:

تواجه البنية التحتية للاتصالات في أغلب دولنا العربية العديد من

المشكلات، إضافة إلى مشكلة الثمن المرتفع لموجات التردد، مما يجعل معظم الشركات لا تملك الإمكانيات المادية لشراء مساحة كبيرة من هذه الموجات، مما يزيد من بطء شبكة الإنترنت ويجعلها غير عملية.

مع الأخذ في الاعتبار التطور التي تمر به الدول العربية لتتغلب على هذه المشكلات والتوجه نحو زيادة وتشجيع التجارة الإلكترونية .

ويستغل كثير من الأشخاص العيوب التي تظهر في التقنية، الأمر الذي يوجد معه مجال كبير للمخاطرة في التجارة الإلكترونية، مثلها مثل المخاطرة في أي مجال تجاري آخر، حيث تنتشر عمليات الاحتيال، وتزييف بطاقات الائتمان، واستخدام البيانات الشخصية بشكل غير قانوني، وغير ذلك مما يتطلب وضع أنظمة تقنية صارمة للحماية التجارية عبر شبكة الإنترنت.

3 - العقبات المالية:

تفتقر معظم الدول العربية لثقافة الكروت الائتمانية، وهي أحد العناصر الأساسية في انتشار التجارة الإلكترونية لسببين رئيسيين: أولهما القواعد المتشددة وعدم الثقة المحيطة باستخراج الكروت الائتمانية، وثانيهما: غياب الوعي بفوائد الاستغناء عن النقود، إضافة إلى غياب تأمين المعاملات الإلكترونية، فرغم أن بعض البنوك توفر هذه الخدمة عن طريق استخراج كروت ائتمانية محدودة الرصيد، إلا أن اتجاه البنوك الاستثمارية إلى طرح أعداد كبيرة من كروت الائتمان على عملائها يمكن أن يساهم في انتشار التجارة الإلكترونية في وقت لاحق.

ويرى بعض الخبراء أن التجارة الإلكترونية تكون أكثر إفادة أثناء الأزمات بصفة خاصة، لأنها تقلل مصاريف الشحن والتخزين للشركات

وبالتالي تنخفض أسعار البضائع.[1]

4 - العقبات الحكومية:

غياب إستراتيجية وطنية للتعامل مع تكنولوجيا الاتصالات وتبني المجتمع لها يشكل عقبة رئيسية أمام التقدم في هذا المجال، بالإضافة إلى اعتماد الحكومة على العمل اليدوي والبيروقراطية وغياب التنسيق بين الجهات الحكومية المختلفة، وعدم وجود قوانين تجارية واضحة، كل هذه العناصر تمثل عقبات أمام تنمية التجارة الإلكترونية في الوطن العربي.

ومع ذلك نجد أن الحكومات بدأت في التفكير بجدية في التحول للعمل الإلكتروني، فشاهدنا ظهور العديد من الحكومات الإلكترونية في الدول العربية، وفي مصر, على سبيل المثال, نرى أن الحكومة تتجه نحو تذليل هذه العقبة مع اتجاهها نحو إنشاء بوابة إلكترونية لها[2] تقدم من خلالها مجموعة من الخدمات للمواطنين, وكذا الحال في دولة الإمارات العربية المتحدة والتي قطعت شوطا كبيراً في التحول إلى الحكومة الإلكترونبة, وهناك مشروع قانون قيد الدراسة ينظم عمل هذه الحكومة.[3]

---

(1) إلا أن بعض الخبراء حذروا من أن الأزمة العالمية التي يمر بها العالم (2008، 2009) قد تؤثر سلبًا بشكل ضئيل في التجارة الإلكترونية؛ لأنها تحتاج لتوفر السيولة وهو الأمر الذي لم يعد متاحًا بشكل كبير بالنسبة للبنوك العالمية. http://www.emaratalyoum.com

(2) www.egypt.gov.eg

(3) راجع دراسة ليونس عرب منشورة في مجلة البنوك في الأردن الأعداد 7، 8، 9، 1999.
تجدر الإشارة إلى أن العديد من الدول العربية (مصر ولبنان والأردن والمغرب والجزائر وتونس وسوريا) وقعت اتفاق تعاون مع الاتحاد الأوروبي ضمن برنامج (يو ميديس) الذي يهدف إلى ردم الهوة الفاصلة بين التقدم في مجتمع المعلوماتية في أوروبا وبين دول حوض البحر الأبيض المتوسط. د. عبد الله الخروم، بحث=

5 - العقبات الاجتماعية:

تعتبر شبكة الإنترنت وسيلة موفرة للوقت والنقود أكثر من أساليب الاتصال الأخرى مثل التليفون والبريد، إلا أن أغلب المستهلكين مازالوا يفتقدون الوعي بفوائد شبكة الإنترنت، وينطبق ذلك على الأفراد والمؤسسات التجارية معًا.

ويفتقر أغلب مستخدمي شبكة الإنترنت في الدول العربية إلى الثقة في المعاملات النقدية من خلال شبكة الإنترنت، نتيجة لغياب الوعي بالقواعد الأمنية على شبكة الإنترنت، أو نتيجة للمقاومة النفسية للتغيير بصفة عامة، فالناس معتادون على التعامل النقدي المباشر، وقد يكون هذا هو السبب في نجاح المواقع التي تسمح بتسجيل الطلب على الموقع، على أن يكون الدفع عند وصول الطلب، كما تعد الأمية عائقًا مهمًّا يقف في طريق أي نوع من أنواع التقدم العلمي والتكنولوجي في الوطن العربي.(1)

= حول قانون المعاملات الإلكترونية الأردني لعام 2001 وأثره في عمليات البنوك، ص 7. www.arablawinfo.com

(1) وأشارت دراسة منشورة على شبكة الإنترنت إلى أن من المعوقات التي تحدّ من تقدم شبكة الإنترنت في العالم العربي وترقيتها إلى المستويات العالميّة: أولا: البنية التحتية، حيث توصلت دراسة أجريت في مصر- إلى أنّ تكلفة تطوير البنية التحتية لتناسب تلك المفترضة تصل إلى 15 مليار دولار أميركي، بينما يتمّ استثمار ما مقداره 0.2% من إجمالي العائدات الوطنيّة للمنطقة في هذا المجال. ثانيا: نوعيّة المحتوى: ويمكن ملاحظة هذه المشكلة بتصفح الكثير من المواقع العربية للمعلومات والأخبار، حيث تقوم معظمها بنشر المعلومات نفسها، نظرا لأنّ أغلبها يقوم بترجمة المعلومات من مصادر عالمية، أو نقلها عن هيئات الأنباء العربية، كما أنّ الكثير من محتوى الجرائد والمجلات الإلكترونيّة يماثل المحتوى الموجود في النسخ الورقية، ولا يتمّ إضافة عناصر التفاعل مع المستخدمين أو إضافة أيّ صور أو عروض فيديو إلى المواقع. ثالثا: عوامل تشريعيّة: ما تزال الكثير من البلدان =

إن تشجيع التجارة الإلكترونية العربية وفتح الباب على مصراعيه أمام الدخول بقوة وجرأة إلى عالم الاقتصاد الجديد، ومن ثم تقليص الفجوة القائمة بين الوطن العربي والعالم الآخر المتقدم، هو أمر محكوم باتخاذ العديد من الخطوات والمتطلبات، وبذل الجهود بصورة جادة وحقيقية، حتى تساهم هذه النوعية الحديثة من التجارة في زيادة حجم التبادل التجاري بين الدول العربية وبقية دول العالم من خلال علاج أوجه القصور وتعظيم الاستفادة من المزايا والفرص المتاحة، بما ينعكس في النهاية على نهضة الاقتصاد القومي العربي وارتفاع مستوى معيشة المواطنين.

ويمكننا تلخيص أهم هذه الخطوات في تطوير البنية الأساسية، ونشر خدمات شبكة الإنترنت، وإيجاد بيئة آمنة للتعاملات الإلكترونية، ومن ثم التوجه إلى الإدارة الإلكترونية، ناهيك عن ضرورة زيادة الإنفاق العربي على البحث العلمي[1]، وأخيراً ضرورة تطوير التشريعات القانونية والتنظيمية من أجل الوصول إلى خلق بيئة مثالية للتجارة الإلكترونية.

= العربيّة تتحكم بالمحتوى الذي يمكن نشره من الناحية الأمنية، الأمر الذي يؤثر على محتوى الصفحات العربية ودور النشر والطباعة حسب كلّ بلد، وتعد تونس هي أول بلد عربي أدخل شبكة الإنترنت عبر 7 شركات حكوميّة لتقديم الخدمات و5 شركات خاصّة.

www.albawaba.com/ar/literature,lterary_Inalysis/276136

(1) حسن الحفني، التجارة الإلكترونية في الوطن العربي الفرص والتحديات، سلسلة دراسات اقتصادية، مركز الخليج للدراسات الإستراتيجية، مايو 2002، ص 91.

المطلب الثالث

مستقبل التجارة الإلكترونية

يتوقع للتجارة الإلكترونية أن تظل في نموها وازدهارها إلى أن تهيمن على جميع الأعمال، وتدخل في جميع الصناعات، وتؤثر على عملية بيع جميع السلع والخدمات وطرق تسويقها، بل تؤثر على شكل الأسواق نفسها وطرق الوصول إليها، وسوف تؤدي إلى خروج البعض من دائرة الأعمال، وإعادة هيكلة العديد من الصناعات، وكذلك ظهور العديد من الصناعات والأعمال الجديدة، فالتجارة الإلكترونية لن تكتفي بأن تكون مجرد طريقة أو وسيلة لبيع السلع والخدمات، بل إنها سوف تزدهر إلى أن تحدث ثورة جديدة تؤثر على شكل الحياة في العالم بأكمله[1].

وفيما يلي بعض السمات المميزة للتجارة الإلكترونية في المستقبل:

أولا: ازدياد أهمية شبكة الإنترنت كوسيلة لانتشار التجارة الإلكترونية:

تظل شبكة الإنترنت هي الوسيلة الأساسية لانتشار التجارة الإلكترونية؛ حيث إنها تعتبر أسرع وسيلة تم تزايد حجمها وعدد مستخدميها مقارنة بالوسائل الأخرى، وقد سبق وأن رأينا كيف نجحت شبكة الإنترنت في أن تصل إلى عشرة مليون مستخدم لها في أربع سنوات فقط، في حين استغرق الهاتف حوالي أربعين عامًا، كما استغرق الفاكس عشرين عامًا لكي يقوم بهذه المهمة، وحتى أنظمة التليفون المحمول فقد استغرقت عشرة أعوام للقيام بهذه المهمة.

(1) **Alex Birch& Others، the age of E،conquering the new world of electronic shopping، U K:OC &C and the Mckrenna Group،2000،P.7.**

ويزيد انتشار استخدام شبكة الإنترنت بشكل ملحوظ، حيث وصل عدد مستخدميها في العالم إلى 349 مليون مستخدم في العام 2000[1]، وقد زاد هذا العدد إلى أكثر من 600 مليون مستخدم في نهاية عام 2002[2]، وإلى 941 مليون مستخدم عام 2005[3].

كما انتشر استخدام شبكة الإنترنت عبر الأجهزة الرقمية المختلفة، فلم يقتصر الأمر على استخدام الحاسبات الشخصية فقط، بل امتد إلى استخدام الأجهزة المحمولة وخاصة التليفون المحمول وكذلك التلفزيون، الأمر الذي أدى إلى سهولة الدخول على شبكة الإنترنت باستخدام أي جهاز رقمي متاح[4].

كما أن هناك اهتمامًا متزايدًا بتطوير الوسائل التكنولوجية المستخدمة، وكذلك شبكات الاتصالات والبنية الأساسية التي تتعلق بزيادة كفاءة وسرعة الإنترنت، فقد زادت الاستثمارات في مجال إدخال سبل جديدة لزيادة كفاءة سرعة الاتصال على شبكة الإنترنت وهو ما يعرف بتكنولوجيا الاتصالات واسعة النطاق، وكذلك استخدام الأقمار الصناعية في عملية الاتصال، الأمر الذي سوف يؤدي إلى القضاء على مشكلة البطء وعدم قابلية الدخول على شبكة الإنترنت، وعلى الاختناقات التي تحدث نتيجة لزيادة عدد المستخدمين

(1) مركز المعلومات ودعم اتخاذ القرار المصري، تقرير عن عدد مستخدمي شبكة الإنترنت في العالم، ص 5.

(2) Elaine X.Grant A study on "E،Commerce to top $ trillion in 2002" OP.Cit.،Pp.11

(3) IDC Corp. By 2005 there will be 941 million user accessing the internet. www. IDC.com/press/research.html.march 13،2002،P،1.

(4) Elaine X.Grant A study on "E،Commerce to top $ trillion in 2002" OP.Cit.،Pp.20، 21.

في وقت معين عن الطاقة القصوى التي تستطيع الشبكة تحملها.

ثانيًا: استمرار تركز الحجم الأكبر من التجارة الإلكترونية بالولايات المتحدة الأمريكية:

تركزت التجارة الإلكترونية منذ بداية ظهورها بالولايات المتحدة الأمريكية، وأصبحت الولايات المتحدة هي القائدة لحركتها في العالم، ويرجع ذلك إلى أن الولايات المتحدة الأمريكية كانت هي مقر ظهور شبكة الإنترنت كما أنه على هذا الأساس انتشرت العديد من الصناعات ذات الصلة بشبكة الإنترنت في الولايات المتحدة، وعلى صعيد المستهلكين فقد أدت سياسة عدم دفع مقابل المكالمات المحلية في الولايات المتحدة، وكذلك انخفاض أسعار الحاسبات الشخصية إلى انتشار استخدام شبكة الإنترنت على مستوى المواطنين.

ومازالت الولايات المتحدة الأمريكية تمثل السوق الأولى للتجارة الإلكترونية سواء على مستوى البائعين أو على مستوى المشترين، بالرغم من محاولات العديد من الدول وخاصة في أوروبا اللحاق بالركب والتقدم في هذا المجال.

ويتوقع أن تظل الولايات المتحدة الأمريكية تحتل المركز الأول في سوق التجارة الإلكترونية في المستقبل المنظور، حيث إن هذا المجال مازال يجذب المستثمرين للتوسع في الصناعات ذات الصلة المباشرة بالتجارة الإلكترونية، مثل الاستثمار في مجال الاتصالات، وبرامج الحاسبات الآلية، والدعاية والإعلان، ومجال التشفير والتأمين، وكذلك مجال شركات بطاقات الائتمان، وكل ذلك من أجل سرعة التكيف مع ما قد يحدث من تطورات في المستقبل.

ويتوقع أن تلحق الدول الأوروبية بالولايات المتحدة الأمريكية ولكن في

مراكز تالية، حيث إنها تحاول حاليًا التغلب على العقبات التي تواجه تقدمها في هذا المجال، مثل ارتفاع أسعار الدخول على شبكة الإنترنت في الدول الأوروبية باستثناء المملكة المتحدة.

كما أن العديد من المشروعات الأمريكية الخاصة بالتجارة الإلكترونية بدأت تنزح إلى الدول الأوروبية مما سوف يساعد على سرعة انتشارها بأوروبا ولكن بأيد أمريكية أيضًا.[1]

---

(1) تتجاوز استثمارات معاملات التجارة الإلكترونية العربية 7 مليار دولار، فيما توقعت دراسة أعدها مجلس الوحدة الاقتصادية العربية أن يتعدى حجم التجارة الإلكترونية وفقًا للإحصاءات الدولية 1000 مليار دولار تقريبًا، ولقد تجاوز حجم التجارة الإلكترونية في دول مجلس التعاون الخليجي 22 مليار درهم (6 مليارات دولار أميركي). فيما قدر معدل نمو التجارة الإلكترونية فيها بنحو 15% سنويا مقابل 300% عالميا. في العام 2008. http://www.albayan.ae

وكان من المتوقع أنه بنهاية عام 2006 أن تكون قد وصلت معدلات التجارة الإلكترونية عربيا إلى 50 مليار دولار، وأن تتفوق فيها دول مجلس التعاون الخليجي مثل الإمارات والسعودية والبحرين وعمان وقطر، وقد أشارت هذه الدراسة الاقتصادية إلى أن حجم التجارة الإلكترونية بين القطاعات التجارية والمستهلكين في دول مجلس التعاون الخليجي يقدر بـ 480 مليون دولار.

كما جاء في دراسة صادرة عن مجموعة (غارتنر غروب) أن معظم بلدان مجلس التعاون الخليجي بصدد خفض تكاليف الاتصال في الوقت الراهن، وأشارت الدراسة إلى أن الدول الخليجية تشهد مستويات عالية في زيادة الاشتراكات مبينة أن مجموع أعداد مستخدمي شبكة الإنترنت في المنطقة سيتضاعف على أقل تقدير بحلول منتصف العام الحالي، وأنه بالإمكان افتراض أن قيمة التجارة الإلكترونية بين القطاعات التجارية والمستهلكين سترتفع إلى نحو مليار دولار بنهاية العام الحالي، كما توقعت أن يمثل مجموع التجارة الإلكترونية في دول مجلس التعاون الخليجي مع نهاية العام الحالي قرابة 10 في المائة من حجم التجارة الإلكترونية الإجمالي، ولقد قدر معدل النمو في التجارة الإلكترونية العربية بنحو 51% مقابل=

ثالثًا: تفوق حجم التجارة الإلكترونية بين وحدات الأعمال بعضها بعضًا (B to B) على حجم التجارة الإلكترونية بين وحدات الأعمال والمستهلكين (B to C):

يتفوق حجم التجارة الإلكترونية حاليًا بين وحدات الأعمال بعضها بعضًا (B to B) على التجارة الإلكترونية بين وحدات الأعمال والمستهلكين (B to C)، حيث وصل حجم التجارة الإلكترونية بين وحدات الأعمال بعضها بعضًا إلى 433 بليون دولار عام 2000(1).

ويتوقع أن يستمر تفوق حجم التجارة الإلكترونية بين وحدات الأعمال بعضها بعضًا عن حجمها بين وحدات الأعمال والمستهلكين في المستقبل، بالرغم من الزيادة التي سوف تحققها كذلك هذه الأخيرة

كما يتوقع أيضًا أنه بحلول عام 2010 سوف تصل نسبة المشتريات التي يقوم بها المستهلكون على شبكة الإنترنت من 10% إلى 50% من حجم المشتريات الكلي في العالم.

رابعًا: عدم خضوع المشترين باستخدام التجارة الإلكترونية لشروط معينة:

يستخدم جميع المستهلكين التجارة الإلكترونية لشراء حاجاتهم اليومية من السلع والخدمات دون التقيد بشروط أو صفات معينة تميز مشتريها عن باقي المستهلكين، ففي بداية استخدام شبكة الإنترنت كانت الغلبة للشباب الذكور

= 3% عالميا مع الإشارة إلى أن حجم التجارة الإلكترونية في الدول العربية يتراوح حاليا ما بين 3 و4 مليارات دولار مقارنة بنحو 631 مليار دولار عالميا. صحيفة البيان الإماراتية في 2005/12/17 .http://www.albayan.ae

(1) Elaine X.Grant A study on "E،Commerce to top $ trillion in 2002" OP.Cit.،Pp.4

المتخصصين في مجالات التقنية الحديثة، أما الآن فإن ثلثي مستخدمي شبكة الإنترنت بغرض الشراء في الولايات المتحدة الأمريكية يزيد سنهم عن الأربعين عامًا، كما أن عدد الذكور يساوي تقريبًا عدد الإناث الذين يقومون بالشراء عبر الشبكة، ومن هنا فيتوقع أن يتأثر جميع سكان العالم بالتجارة الإلكترونية دون تفرقة بسبب العمر أو الجنس.

خامسًا: تأثير التجارة الإلكترونية على جميع السلع والخدمات:

تؤثر التجارة الإلكترونية على جميع السلع والخدمات، وخاصة الحاسبات الآلية الشخصية (P.C) وبرامج الحاسبات والموسيقى والكتب وتذاكر الطيران، حيث إن هذه السلع والخدمات تمثل حاليًا 80% مما يباع باستخدام التجارة الإلكترونية، ولكن الأمر لن يقتصر على هذه الفئات فحسب، بل يتوقع أن تشمل التجارة الإلكترونية بيع الملابس والهدايا والسيارات حتى تحتل هذه الفئات مراكز متقدمة في حجم المبيعات المحققة عبر شبكة الإنترنت، بالإضافة إلى النمو المتزايد الذي سوف يشهده بيع تذاكر المناسبات الخاصة والاحتفالات، ولعب الأطفال والمنتجات الصحية والأدوات المستخدمة في الحدائق عن طريق التجارة الإلكترونية في المستقبل[1].

وفي النهاية فإن التجارة الإلكترونية تعد أداة لزيادة القدرة التنافسية[2] بما توفره من أدوات ووسائل تزيد القدرة التنافسية للمنتجين، بما يمكنهم من تحقيق زيادة صادراتهم بإتاحة وتسهيل الوصول إلى مراكز الاستهلاك الرئيسية، وتسويق السلع والخدمات عالميًا بتكلفة محدودة، وسرعة عقد

(1) هند محمد حامد، التجارة الإلكترونية في المجال السياحي، مرجع سابق، ص45.

(2) د. حمدي عبد العظيم، أبعاد التجارة الإلكترونية، مجلة البحوث الإدارية، العدد الأول، يناير 2001، ص7.

وإنهاء الصفقات، والقدرة على تحديد الأسواق، والاستجابة لتعزيز طلبات المستهلكين، وتنشيط المشروعات المتوسطة والصغيرة من خلال المشاركة في حركة التجارة العالمية بفاعلية وكفاءة، نظرًا لانخفاض تكاليف التسويق والدعاية والإعلان.

كما أنها ينتج عنها خلق فرص جديدة للعمل الحر، بفضل ما تتيحه من فرص لعمل مشروع تجاري متصل مباشرة بالأسواق العالمية بتكلفة بسيطة، وتصدير إنتاجه إلى تلك الأسواق العالمية، كما أنها أداة لنقل التكنولوجيا بما توفره من تقنيات عالية إلى كافة المشاركين فيها، وإجمالا فهي تؤدي إلى تقليل نفقات الإنتاج والتسويق، وسرعة إنجاز الصفقات، وتعظيم الربح، مع تزايد جو الثقة والأمان في التعاملات التجارية[1].

ومما يدلل على ذلك ما أكدته الجمعية العامة للأمم المتحدة في ديباجة قرارها رقم 51 /162 الصادر في 1996/12/16 بإصدار قانون اليونسترال النموذجي بشأن التجارة الإلكترونية بإقرار التبادل الإلكتروني للبيانات باعتباره بدائل للأشكال الورقية للاتصال وتخزين المعلومات، وفي تأكيد مؤتمر الأمم المتحدة للتجارة والتنمية على تقرير البنك الدولي من أن الكيانات التي لا يتوافر لها إمكانيات التبادل الإلكتروني للمعلومات سيكون نصيبها من التجارة الدولية هو الإخفاق والخروج من مجالها[2].

(1) د. السيد أحمد عبد الخالق، الأهمية الاقتصادية للتجارة الإلكترونية، جامعة المنصورة، ص 325.
(2) مؤتمر الأمم المتحدة للتجارة والتنمية (الإنكتاد)، التجارة الإلكترونية اعتبارات قانونية، 1998/5/15.

الفصل الثاني

الحماية القانونية للتجارة الإلكترونية

تمهيد وتقسيم:

تمثل الجريمة اعتداءً على مصلحة يرى المشرع أنها جديرة بالحماية ويجرم الاعتداء عليها، والمشرع الجنائي يقدر أهمية التجارة الإلكترونية ويحمي حرية ممارستها في أمان وبعيدًا عن التحايل؛ لذلك ينص على تجريم أفعال تمثل اعتداءً من وجهة نظره على ممارسة هذه التجارة من خلال شبكة الإنترنت، والقانون النموذجي للأمم المتحدة المتعلق بالتجارة الإلكترونية يقرر أن هذه الحماية تتعلق بكل ما يمس الأنشطة التجارية.

كما يحمي المشرع في التجارة الإلكترونية عدة مصالح، فالمادة الأولى من القانون النموذجي للأمم المتحدة تنص على نطاق التطبيق حيث تقرر أن هذا القانون ينطبق على أي نوع من المعلومات تكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية[1]، وقد يتأتى الاعتداء على هذه المصالح من عدة أطراف، كأن يصدر عن العميل أو التاجر أو طرف ثالث من الغير، وسوف نعرض لمفهوم الحماية القانونية للتجارة الإلكترونية من خلال مبحثين: الأول المصلحة المحمية في التجارة الإلكترونية، والثاني صور الحماية القانونية للتجارة الإلكترونية.

المبحث الأول: المصلحة المحمية في التجارة الإلكترونية

المبحث الثاني: صور الحماية المختلفة للتجارة الالكترونية.

---

(1) Article 1. Sphere of application: This Law applies to any kind of information in the form of a data message used in the context of commercial activities.

المبحث الأول

المصلحة المحمية في التجارة الإلكترونية

تعرف المصلحة بأنها عبارة عن وصف مستقر في النظام الاجتماعي، يترتب على وجودها وإقرارها سلسلة متصلة من المنافع، وأساس المصلحة هي القاعدة الاجتماعية الاقتصادية فالمصالح على هذا النحو تعد دستور النظام الاجتماعي الذي يعمل المجتمع على حمايته، ومن هذه المصالح ما يتميز بطابع خاص يبرر وضع مجموعة نصوص خاصة به لتكون نظامًا مستقلا إلى حد ما عن قانون العقوبات[1].

وفي التجارة الإلكترونية تتعدد المصالح المحمية لتأمين ممارسة وتداول السلع والخدمات عبر شبكة الإنترنت، ويقود موضوع المصلحة المحمية بشكل أو بآخر إلى حمايتها، ويتفق الفقه الجنائي على أن القانون الجنائي من حيث طبيعته يعبر عن حماية المصلحة المقررة القائمة والمشروعة للنظام الاجتماعي الاقتصادي، وإن كان الفقه قد اختلف في تحديد أسس العدوان على هذه المصلحة، فهو إما أنه تعبير عن خلل في النظام الاجتماعي الاقتصادي، وإما أنه نتيجة لظروف اجتماعية اقتصادية - وأحيانا سياسية - دون أن يكون للنظام الاجتماعي الاقتصادي أدنى تأثير في إحداثه أو في وجوده.[2]

وعلى كل حال فإن هناك ترابطًا بين المصلحة والحماية الجنائية، إذ ليس هناك نص أو قاعدة قانونية خالية من الغاية التي يستهدفها المشرع

(1) د. محمود محمود مصطفى، الجرائم الاقتصادية في القانون المقارن، الأحكام العامة والإجراءات الجنائية، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، ص 6.

(2) د. عبود السراج، الجريمة في إطار التفسير الاقتصادي للمجتمع، مجلة الحقوق والشريعة، العدد الثاني السنة الثالثة، الكويت 1979، ص 126.

وهي تنظيمها وحمايتها.[1]

وسوف نتعرض لهذا الموضوع من خلال ثلاثة مطالب:

المطلب الأول: وجود المصلحة المحمية وأوجهها

المطلب الثاني: الحماية الجنائية لأطراف عقود التجارة الإلكترونية

المطلب الثالث: حماية وسائل الدفع الإلكتروني.

المطلب الأول

وجود المصلحة المحمية وأوجهها

الحماية والرعاية للمصالح هي الوظيفة الرئيسية المناطة بالنظام القانوني في أي مجتمع، ويتكون هذا الأخير من مجموعة من المصالح القائمة والمشروعة في الواقع الاجتماعي وبعنصريه المادي والمعنوي.

وتختلف النظم الاجتماعية والاقتصادية من دولة إلى أخرى، الأمر الذي يؤدي إلى اختلاف المصالح القائمة والمشروعة، ويترتب على ذلك اختلاف أشكال تنظيم وتطوير ورعاية تلك المصالح، ومن ثم اختلاف النظم القانونية.

ويعد القانون الجنائي إحدى الوسائل الشرعية لتشييد معالم النظام الجنائي، الذي يتولى بدوره تقرير الحماية الجنائية لمجموع المصالح القائمة والمشروعة في القاعدة الاجتماعية الاقتصادية، ومن ثم فإنه من غير المتصور بحث القانون الجنائي دون أن يسبق ذلك بحث في النظام القانوني، ولهذا الأمر أهميته حيث ينتهي إلى ضرورة توءمة النظام الجنائي بالتفاعل الحادث في فروع النظام القانوني تجنبًا للخلل في الأخير، وهذا الأمر

(1) د. مأمون محمد سلامة، بحث بعنوان قانون العقوبات بين الفكر المحافظ والفكر المتطور، دراسات قانونية, كلية الحقوق, الجامعة الليبية, 1971، ص 48.

يستدعي بالضرورة الإلمام بالفروع الأخرى للنظام القانوني، وكذلك الإحاطة بالنظام الاجتماعي الاقتصادي وما يحويه من مصالح قائمة ومشروعة.[1]

وينبغي حين التعرض بالدراسة للحماية الجنائية لموضوع ما أن يتم بحث المصلحة محل الحماية الجنائية التي تمثل الموضوع القانوني للجريمة، في محاولة لرسم معالم النموذج الإجرامي، توصلا إلى تحديد دقيق للموضوع المادي للسلوك الإجرامي الذي يتم به العدوان على المصلحة المذكورة مع ما يترتب على ذلك من نتائج.

وسنتناول في هذا المطلب وجود المصلحة المحمية واستحداثها، ثم نبين أوجه هذه المصلحة المحمية في التجارة الإلكترونية، والتي تتمثل في شرعية تداول البيانات الإلكترونية، وسرية هذه البيانات وخصوصيتها، وحماية التعاقد والتوقيع الإلكتروني، وحماية المستهلك الإلكتروني من الغش والتحايل، وحماية أسماء الدومين وحقوق الملكية الفكرية، وذلك وفقًا للتفصيل التالي.

الفرع الأول

وجود المصلحة واستحداثها

إذا أراد صاحب حق المطالبة بحقه أمام القضاء، وجب أن يكون له مصلحة في ذلك قبل رفعه لهذه الدعوى، والمصلحة المعنية هنا هي ذلك الحق أو المركز القانوني محل الاعتداء.

ولأن الدعوى تعد وسيلة لحماية هذا المركز القانوني أو الحق، فينبغي

(1) د. عمر محمد بن يونس، الحماية الجنائية للثروة النفطية، دار الفكر الجامعي، 2004، ص 91.

أن يكون هذا المركز القانوني أو الحق قائمًا، ولذلك اعتبر الفقه هذا الشرط وهو قانونية المصلحة أو قانونية الدعوى، فلابد أن يكون القانون معترفًا بالحماية المجردة لنوع المصلحة التي يطلبها المدعي.

ولذلك يمكن القول بأن المصلحة هي الفائدة العملية التي تعود على المدعي من الحكم في دعواه، يستوي في ذلك أن تكون المصلحة مادية أو معنوية.

والمصلحة المادية هي التي تحمي المنفعة المادية لرافع الدعوى، أما المصلحة الأدبية فهي التي تتعلق بالتعويض عن الإساءة لاعتبار الشخص في شرفه أو آلامه النفسية، وإذا ما تبين للقاضي أن الحق أو المركز القانوني لا يقره القانون ولا يحميه، فهو يقضي بعدم قبول الدعوى لعدم قانونيته.[1]

وقد أثار الفقيه الإيطالي جاروفالو R. Garofalo[2] موضوع المصالح الطبيعية وتلك المصطنعة، وذلك إزاء تقسيمه للعدوان الإجرامي إلى جرائم طبيعية ومصطنعة.

وعلى الرغم من النقد الذي تعرض له جاروفالو في إطار تقسيمه السابق، إلا أن أيًّا من تلك الانتقادات لم تصب هذه الفكرة بضرر، وبناءً على هذه الفكرة فقد وضعت البذور الأولى حول قابلية المصالح في القانون الجنائي للانقسام إلى طبيعية ومصطنعة.

ووفقًا لهذا التصور فإن المجتمعات البشرية عرفت المصالح المحمية في

(1) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 268.

(2) الفقيه الايطالي جاروفالو R. Garofalo (1851، 1943) أبرز فكرته بشأن الجريمة الطبيعية (والجريمة المصطنعة) في نهاية القرن التاسع عشر.

مراحلها القديمة، وقبل أن تقوم وتستقر فيها مفاهيم الشعوبية ومدلول الملكية والكتابة، وأخضعت هذه المجتمعات العدوان عليها لجزاء بدائي قائم على العرف السائد أي قانون ما قبل نشأة التاريخ المكتوب، في حين أن هناك مصالح أخرى لم تتواجد إلا في مرحلة حديثة نسبيًا، سيما بعد ظهور فكرة الدولة، وما تبع ذلك من إرساء للنظام الاجتماعي الاقتصادي فيها، وهي مصالح لم تكن معروفة من قبل، وترتب على ذلك أن وجدت صور للمساس بتلك المصالح تختلف في الجملة عن المساس التقليدي.

وفي رأينا أن تقسيم جاروفالو الجرائم إلى طبيعية ومصطنعة يوجد له أساس منطقي، بمعنى أنه كلما وجدت الدولة وجد التجريم المصطنع، أي استحداث الجرائم ترتيبًا على استحداث المصالح المتناسبة مع مكونات النظام الاجتماعي الاقتصادي، في حين أن الجريمة الطبيعية ليست سوى تطبيق للقاعدة القديمة في أصل الجريمة.

والجريمة في نطاق التجارة الإلكترونية تضر بأطراف عديدة، وتصيب مصلحة كل منهم سواء أكان البائع أم المشتري، وكذلك المنتج والمستهلك، وهو الأمر الذي حاول واضعو القانون النموذجي للأمم المتحدة التنبيه إليه بأن المساس بالمصلحة في نطاق التجارة الإلكترونية يتحقق من خلال الاعتداء على كل ما يتعلق بالأنشطة التجارية.[1]

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 15.

الفرع الثاني

أوجه المصلحة المحمية

تمثل الجريمة كما رأينا اعتداءً على مصلحة يحميها القانون ويرى المشرع أنها جديرة بالحماية التشريعية، وينص على حمايتها نظرًا لأهميتها، ويجرم الاعتداء عليها[1]، وهو في التجارة الإلكترونية إنما يحمي حرية ممارسة هذه التجارة في أمان وبعيدًا عن التحايل، لذلك ينص على جرائم تمثل اعتداءً من وجهة نظره على ممارسة هذه التجارة من خلال شبكة الإنترنت، لذلك جاء نص القانون النموذجي للأمم المتحدة المتعلق بالتجارة الإلكترونية على أنها تتعلق بكل ما يمس التجارة.

وتتمثل معظم المصالح المحمية في التجارة الإلكترونية في شرعية تداول البيانات، وسريتها، وخصوصيتها، وحماية التعاقد والتوقيع الإلكتروني، وحماية المستهلك من الغش المعلوماتي، وحماية أسماء الحقول، وحقوق الملكية الفكرية، وذلك على التفصيل التالي.[2]

1 - شرعية تداول البيانات الإلكترونية:

تتمثل هذه المصلحة المحمية في ضرورة أن يتم تداول البيانات بشكل مشروع، وأن يتم تداولها ممن له الحق في التداول والاستخدام، وقد عبر القانون النموذجي للأمم المتحدة الخاص بالتجارة الإلكترونية في المادة 2/ب بأنه يراد بمصطلح "تبادل البيانات الإلكترونية" نقل المعلومات إلكترونيًا من

(1) د. محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، الطبعة العاشرة، دار النهضة العربية، القاهرة، 1984، ص6.

(2) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 15.

حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لإنشاء المعلومات، ويشترط أن يتم تداول البيانات عن طريق مزود الخدمة الإلكترونية المصرح له بذلك[1].

وعملية التجارة تمثل تعاملا بالبيع والشراء بين بائع ومشتر بمفهوم business to business، والتسوق الإلكتروني والتعاملات المصرفية online banking، والبيانات التي يمكن إرسالها إلكترونيًا وطلبات الشراء والبيع ومشرعات التعاقد.

والتجارة الإلكترونية تعتمد أساسًا على تبادل البيانات إلكترونيا electronic data interchange ويعتمد تبادل البيانات إلكترونيًا على شبكة القيمة المضافة "VAN" value added network التي تقوم بتجميع البيانات من عدة فروع لمعرفة طلبات الشراء، وإرسال تلك البيانات إلى صندوق بريد إلكتروني يسمح بالاتصال المباشر بحواسب العملاء، وبالتالي حرية تبادل البيانات على نطاق واسع، وفتح أسواق لحركة التجارة، وقد تتعلق البيانات بالتعاقد أو شرط البيع أو الثمن، ومن هنا تأتي أهميتها.

ولتخفيض النفقات اتجهت شركات الأعمال إلى تجارة الشبكات مباشرة، وهي التي تيسر للعملاء تبادل المعلومات داخل الشركة من خلال شبكة الإنترنت، أو الإكسترانت وهي تستخدم نفس معايير شبكة الإنترنت لتبادل المعلومات التجارية، وشبكة الإكسترانت[2] تسمح بتبادل البيانات التجارية

(1) T. delugo، La Legislation penala & son application،Uni. De Caire 1956 p. 232

(2) شبكة الإكسترانت هي الشبكة المكوّنة من مجموعة شبكات إنترانت ترتبط ببعضها عن طريق شبكة الإنترنت، وتحافظ على خصوصية كل شبكة إنترانت مع منح أحقية الشراكة على بعض الخدمات والملفات فيما بينها، أي أن شبكة الإكسترانت=

بين الشركاء من خلال بوابة آمنة إلى شبكة الإنترنت، وهي بذلك تستخدم نفس قواعد برتوكول شبكة الإنترنت.[1]

ومن أهم التوصيات الأوروبية في هذا المجال تلك التوصية رقم [46] لسنة 1995 والمعروفة بتوصية [الحياة الخاصة] والمصدق عليها بواسطة البرلمان والمجلس الأوروبي معًا في 24 أكتوبر 1995، والخاصة بحماية الأشخاص الطبيعيين بالنسبة لمعالجة البيانات ذات الصفة الشخصية والخاصة أيضًا بحرية مرور هذه البيانات , والتي تؤكد على ضرورة حماية الحقوق الأساسية وحريات الأفراد, وعلى وجه الخصوص الحق في حرمة الحياة الخاصة, والبيانات الشخصية, والتى حددتها بأنها كل بيان يتعلق بشخص محدد أو قابل للتحديد, بصورة مباشرة أو غير مباشرة, على وجه الخصوص، عن طريق رقمه القومي أو بالرجوع للبيانات المتعلقة

= هي الشبكة التي تربط شبكات الإنترانت الخاصة بالمتعاملين والشركاء والمزودين ومراكز الأبحاث الذين تجمعهم شراكة العمل في مشروع واحد، أو تجمعهم مركزية التخطيط أو الشراكة، وتؤمن لهم تبادل المعلومات والتشارك فيها دون المساس بخصوصية الإنترانت المحلية لكل شركة، وبناءً على التعريف السابق يمكن أن نجد تطبيقات شبكة الإكسترانت في المجالات التالية: نظم تدريب وتعليم العملاء (Clients Training), نظم التشارك على قواعد البيانات بين الجامعات ومراكز الأبحاث التابعة لحكومة ما أو لإدارة معينة, شبكات مؤسسات الخدمات المالية والمصرفية, نظم إدارة شئون الموظفين والموارد للشركات العالمية المتعددة المراكز والفروع...إلخ.
At: http://www.itep.ae/Arabic/EducationalCenter/Articles/Extranet_01.asp

(1) يونس عرب، البنوك الخلوية، التجارة الخلوية، المعطيات الخلوية،M. M، banking، commerce, data،M، ثورة جديدة تنبئ بانطلاق عصرـ ما بعد المعلومات، بحث منشور على شبكة الإنترنت، http://www.arablaw.org

بحالته الصحية أو الاقتصادية أو الثقافية أو الاجتماعية (المادة 2 من التوجيهات).

وتطبيقًا لهذه التوصية فإنها تحمي إنشاء البطاقات ابتداءً من تسجيل البيانات الشخصية على شبكة الإنترنت، وتحمي النقل بواسطة شبكة الإنترنت لبطاقات البيانات الشخصية، كما تحمي تجميع وربط مثل هذه البطاقات المبعثرة على الحاسبات المختلفة المرتبطة بشبكة الإنترنت[1].

وقد أكد التوجيه الأوروبي المشار إليه على حق الفرد في الاطلاع على البيانات المتعلقة به (م 12 منه), وحقه في الاعتراض على أي استخدام لهذه البيانات (م 14), وحقه في سرية هذه البيانات (م 16, 17)[1]، ومن الطبيعي أن حماية هذه البيانات في التشريعات الأوروبية التى سبقت أو تلت هذه التوجيهات ستكون حماية جنائية عند اللزوم بجانب الصور الأخرى للحماية.

كما حرص مجلس أوروبا على التصدي للاستخدام غير المشروع للحاسبات والشبكة المعلوماتية، وجاء ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالجريمة الافتراضية "Convention on cybercrime" Budapest، 2001 والتي نصت على تجريم الولوج غير القانوني، والاعتراض غير القانوني، والاعتداء على سلامة البيانات، وإساءة استخدام أجهزة الحاسب، والتزوير المعلوماتي، والغش المعلوماتي، والجرائم المتصلة بالمواد الإباحية الطفولية، والجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة.[2]

(1) د. محمود السيد عبد المعطي خيال، الإنترنت وبعض الجوانب القانونية، دار النهضة العربية،ص 102.
(2) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، =
= دار النهضة العربية، 2007، ص 5.

2 - سرية البيانات وخصوصيتها:

أصبحت شبكة الإنترنت التي سهلت الكثير من أمور الحياة، وتجاوزت عقبات كثيرة كنا نراها في الماضي من ضروب المستحيل، أصبحت من أخطر آليات التكنولوجيا المعاصرة تهديدًا لحياة الإنسان في أخص شئونها وأكثرها التصاقًا به، ولكون شبكة الإنترنت شبكة غير مملوكة لأحد، فإن باستطاعة أي شخص الولوج إليها والحصول على ما يريد منها، وفي أحيان كثيرة تتطلب بعض المواقع بيانات ومعلومات شخصية للسماح بدخولها، ومن ناحية أخرى فشبكة الإنترنت لا تتوافر فيها السرية الكاملة، والأمان لما ينقل عبرها من معلومات أو بيانات، وقد سهل ذلك الحصول من خلالها على المعلومات والبيانات الخاصة بالأفراد بطريقة غير مشروعة.

بعض البيانات المعالجة المتاحة لمشتركي ومستخدمي شبكة الإنترنت لا تثير أية مشكلات في الاستخدام كالمعلومات العلمية والصحية والمعارف وغيرها، أما البيانات التي تتمتع بالحق في الخصوصية والسرية فيجب احترام هذا الحق في الخصوصية، وقد نص المبدأ الثالث في شأن حماية المستهلك في مشروع قانون التجارة الإلكترونية المصري على ضرورة احترام الحق في سرية البيانات الخاصة بالعملاء واحترام الحق في الخصوصية.[1]

وقد عبر عن ذلك أحد الكتاب الأمريكيين حينما قال: (إن الموظفين في شركات التأمين يعرفون عن تفاصيل الحياة الخاصة أكثر مما يعرفه أي

(1) الخصوصية وحماية البيانات في البيئة العربية، وبحث آخر بعنوان الخصوصية وحماية البيانات، التأليف مجموعة باحثين، البحثان منشوران على شبكة الإنترنت: http://www.arablaw.org

طالب زواج عن الخطيبة التي يعتزم الزواج منها).[1]

كما يستطيع بعض الأشخاص الدخول إلى أنظمة وأجهزة تخص أشخاصًا آخرين والحصول على معلومات عن أسرار حياتهم الخاصة، وأية معلومات أخرى تخصهم قد يرغب صاحبها في إضفاء طابع السرية عليها، أو تلك المعلومات التي تتولد عن حريته في اختيار حياته الخاصة فهي ملك الفرد، وتكمن أسرار الحياة في جسم الإنسان، وفي مكنونه النفسي- والفعلي، وفي الكيان الداخلي كصحته بما في ذلك أمراضه، وفي مكنونه الخارجي كسكنه ومحادثاته أو مراسلاته الشخصية، وذمته المالية، ونشاطه كالمراسلات والصور الخاصة به، وأخبار تحركاته الخاصة والطلاق والزواج والمرض فهي ملك الفرد[2].

والبيانات الشخصية المتصلة بالحياة الخاصة بالفرد أو عائلته غالبًا ما يقدمها الشخص بنفسه، أو قد تتوصل الهيئات أو الأفراد إليها بوسيلة أو بأخرى، وتهديد المساس بالحياة الخاصة قد يثور إذا أفشيت هذه المعلومات دون رضاء منه، أو نشرت بإحدى طرق العلانية دون موافقته، سواء أكانت هذه المعلومات في شكل خبر أو تعليق أو صورة، وتكون متصلة بأسرار حياته الخاصة أو العائلية ولو كانت هذه المعلومات صحيحة.

وتأتي بطاقات الائتمان على قائمة الآليات الأكثر تهديدًا للتاجر والمستهلك في مجال التجارة الإلكترونية، ومن أجل تلافي وجود مخاطر أمنية فإن البنوك والمؤسسات العالمية بالتعاون مع المنظمات المالية المختصة قامت بوضع قواعد ونظم أمنية تتسم بحماية عالية التقنية، بجانب

(1) د. السيد عتيق، جرائم الإنترنت، مرجع سابق، ص 61.
(2) د. طارق فتحي سرور، دروس في جرائم النشر، دار النهضة العربية، 1997، ص 251.

نظم أخرى لحماية المستهلك في إجرائه لعمليات الشراء والبيع، وكذلك حماية التاجر الذي يقوم بعرض السلعة أو الخدمة، وذلك عن طريق رقم مشفر لا يعرفه إلا العميل للحد من التحايل الإلكتروني.[1]

وبالنظر إلى التشريعات المقارنة نجد أن التشريع الفرنسي قد جاء في مقدمة التشريعات الأوروبية التى وفرت حماية جنائية للبيانات الشخصية منذ ثلاثة عقود تقريبًا، حيث صدر قانون 6 يناير سنة 1978 المنظم للمعالجة الرقمية والحريات، وقد تطلب هذا القانون عند معالجة البيانات الشخصية من قبل الأفراد ضرورة إبلاغ اللجنة القومية لمعالجة البيانات والحريات (CNIL)[2], فضلا عن ضرورة إخطارها في حالة تعامل القائمين على أحد مواقع الإنترنت مع البيانات الشخصية، وتخطر اللجنة المواطنين بالمخاطر المرتبطة بوضع بياناتهم الشخصية بموقع الإنترنت, فضلا عن حقهم في الاعتراض على نشرها, وحقهم في الاطلاع عليها, وتصحيحها ومحوها لأسباب مشروعة.

وقد نص قانون 6 يناير سنة 1978على عدد من الجرائم لتوفير الحماية الجنائية للبيانات الشخصية للأفراد, وقد تم إعادة النص على هذه الجرائم في قانون العقوبات الفرنسي الجديد, وذلك في المواد 226-16 إلى 226-24 من القانون, تحت عنوان "الاعتداءات على حقوق الشخص الناتجة عن نظام

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 21.

(2) Xavier Linants de Bellefonds-Alain Hallande, Pratique du droit de l'informatique, 4éme éd. Delmas, 1998, P.240 ; Valerie Sedallien, création d'une site sur l'internet, aspects juridiques. Voir le site: www.internet_juridiques.net

مشار إليه لدى د. محمد أبو العلا عقيدة, الحماية الجنائية للتجارة الإلكترونية, مرجع سابق, ص18.

Fichiers أو المعالجة الرقمية للبيانات, وسنشير بإيجاز لهذه الجرائم:

1) جريمة عدم اتخاذ الإجراءات الأولية لإجراء معالجة البيانات:

تنص على هذه الجريمة المادة 226-16 من قانون العقوبات الفرنسي الجديد بقولها: "كل من باشر- ولو بطريق الإهمال - أو أمر بمباشرة المعالجة الإلكترونية للبيانات الاسمية, دون مراعاة الإجراءات الشكلية المنصوص عليها في القانون للقيام بها, يعاقب بالحبس ثلاث سنوات, والغرامة البالغ مقدارها 45 ألف يورو" من هذه الإجراءات السابقة على القيام بالمعالجة الإلكترونية للبيانات ضرورة إخطار اللجنة القومية لمعالجة البيانات والحريات (CNIL).

2) جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات المعالجة:

تنص على هذه الجريمة المادة 226-17 بقولها: "كل من أجرى أو أمر بإجراء معالجة إلكترونية للبيانات الاسمية دون أن يتخذ الإجراءات الضرورية للحفاظ على هذه البيانات, وعلى وجه الخصوص منع تشويهها أو إتلافها, أو اطلاع الغير غير المصرح له بذلك عليها, يعاقب بالحبس خمس سنوات, وبغرامة مقدارها 300 ألف يورو".

3) جريمة تسجيل وحفظ بيانات شخصية بدون موافقة صريحة من أصحابها:

تنص على هذه الجريمة المادة 226-19 من قانون العقوبات الفرنسي الجديد بقولها: "كل من وضع أو حفظ خلافًا للقانون في ذاكرة إلكترونية بدون موافقة صريحة من صاحب الشأن, بيانات اسمية تظهر بصورة مباشرة أو غير مباشرة أصوله العرقية أو معتقداته السياسية أو الفلسفية أو الدينية أو انتماءاته النقابية, أو تتعلق بأخلاقه, يعاقب بالحبس خمس سنوات, وبغرامة تبلغ 300 ألف يورو.

كما يعاقب بنفس العقوبات كل من وضع أو حفظ في ذاكرة إلكترونية خلافًا للقانون، معلومات اسمية في ذاكرة إلكترونية تتعلق بالجرائم أو أحكام الإدانة أو التدابير الاحترازية".

النص السابق يتضمن في الواقع جريمتين: الأولى: المعالجة غير القانونية للبيانات الاسمية التى تظهر أصول الشخص العرقية أو آراءه السياسية أو الدينية.. إلخ، ويشترط لقيام الجريمة أن تتم دون موافقة صريحة من صاحب الشأن؛ إذ أن موافقته تعد سببًا لإباحة هذه الجريمة.

والجريمة الثانية تتعلق بمعالجة بيانات اسمية خلافًا للقانون، تظهر الجرائم التى ارتكبها شخص معين، أوأحكام الإدانة (عقوبة أم تدبير) الصادرة ضده، حيث يتضمن ذلك تشهيرًا به وإضرارًا بسمعته، وربما تتم هذه المعالجة بعد أن يكون قد رد إليه اعتباره[1].

4) جريمة حفظ بيانات شخصية مدة تتجاوز الوقت المحدد لحفظها:

جاء النص على هذه الجريمة في المادة 226-20 عقوبات فرنسي بقولها: "كل من قام بحفظ معلومات اسمية متجاوزًا بذلك المدة المحددة في طلب الموافقة أو الإخطار السابق على عملية المعالجة، يعاقب بالحبس ثلاث سنوات، وبالغرامة التي تبلغ 45 ألف يورو، ويستثنى من ذلك حالة ما إذا كان الحفظ قد تم لأغراض تاريخية أو إحصائية أو علمية في نطاق الشروط المبينة قانونًا".

وقد تم تعديل هذا النص بالقانون رقم 2000-321 الصادر في 12 أبريل سنة 2000، وبمقارنة النص الحالي بالنص السابق على سنة 2000 يتضح من ناحية أن النص السابق كان يشترط لقيام الجريمة عدم الحصول

(1) د. محمد أبو العلا عقيدة، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص19.

مقدمًا على موافقة اللجنة لمعالجة البيانات وحماية الحريات (CNIL)، ومن ناحية أخرى يتضح أن العقوبات المقررة في النص الحالي أشد من سابقه فيما يتعلق بالغرامة.

5) جريمة المعالجة غير المشروعة للبيانات:

تنص المادة 226- 18 من قانون العقوبات الفرنسي- الجديد على أن: "كل من قام بجمع بيانات بوسيلة الغش أو بطريقة غير أمينة أو غير مشروعة، أو قام بمعالجة البيانات الاسمية لشخص طبيعي رغم معارضته, إذا كانت هذه المعارضة مؤسسة على أسباب مشروعة, يعاقب بالحبس لمدة خمس سنوات, وبغرامة تبلغ 300 ألف يورو".

"إذا كانت معالجة البيانات الاسمية لأغراض تتعلق بالأبحاث في مجالات الصحة فإن الجاني يعاقب بنفس العقوبة السابقة في حالتين: **الأولى:** إذا لم يخطر أصحاب الشأن بحقهم في الاطلاع عليها وتصحيحها أو الاعتراض عليها, وإخطارهم بطبيعة البيانات, ومن سيتلقاها.

الحالة الثانية: إذا كان هناك اعتراض من صاحب الشأن, أو إذا كان القانون ينص على ضرورة توافر موافقة صريحة وواضحة منه, أو إذا تعلق الأمر بشخص توفي اعترض قبل وفاته على معالجة البيانات الخاصة به ".

والفقرة الثانية من النص تريد تشجيع البحث العلمي في المجال الطبي بشرط المحافظة على البيانات الشخصية للمريض الخاضع لمعالجة بياناته حيث اشترطت إخطاره مسبقًا, والحصول على موافقته الصريحة بالمعالجة[1].

---

(1) إذا كان التشريع الفرنسي قد قدم حماية شاملة للبيانات الشخصية منذ سنة 1978, فإن القانون البلجيكي بعد ذلك بعقدين بدءًا من سنة 1999 قد قدم حماية للبيانات=

6) جريمة تغيير الغرض المحدد لجمع البيانات الاسمية:

تنص المادة 226 - 21 على هذه الجريمة بقولها: " كل من يحوز بيانات اسمية بمناسبة تسجيلها أو فهرستها أو نقلها أو تحت أي شكل آخر من أشكال المعالجة, وقام بتغيير الغرض المحدد منها بالنص القانوني أو اللائحة اللذين صرحا بالمعالجة الإلكترونية لهذه البيانات، أو بقرار من اللجنة القومية لمعالجة البيانات وحماية الحريات بالتصريح بمعالجة البيانات لأغراض الأبحاث الطبية, أو بالإخطار المسبق لإجراء معالجة البيانات, يعاقب بالحبس خمس سنوات وبالغرامة التى تبلغ 300 ألف يورو".

7) جريمة إفشاء سرية البيانات الاسمية بما يضر بصاحب الشأن:

تنص على هذه الجريمة المادة 226-22 من قانون العقوبات الفرنسي بقولها: "كل شخص قام بإفشاء سرية البيانات الاسمية, بمناسبة تسجيلها أو فهرستها أو نقلها, أو بأي شكل من أشكال معالجة البيانات الاسمية, إذا ترتب على إفشاء سريتها الإضرار باعتبار الشخص, أو حرمة حياته الخاصة, أو إذا قام دون التصريح من صاحب الشأن بنقل هذه المعلومات إلى الغير الذي ليس صفة في تلقي هذه المعلومات, يعاقب بالحبس لمدة سنة, وبالغرامة التى تبلغ 15 ألف يورو, وتكون العقوبة الغرامة التى تبلغ 7500 يورو إذا تم الكشف عن هذه المعلومات بطريق الخطأ المتمثل في عدم الاحتياط أو الإهمال.

= الشخصية, وذلك بتقييد عملية استخدامها في التسويق المباشر, وفرض التزامًا على الشخص القائم بمعالجة هذه البيانات بإخطار صاحب الشأن بحقه في الاعتراض على البيانات التى يتم جمعها بغرض التسويق المباشر, فضلا عن حقه في الاطلاع عليها وفي تصحيحها. راجع حول ذلك د. مدحت عبد الحليم رمضان, الحماية الجنائية للتجارة الإلكترونية, مرجع سابق, ص 81.

وفي الحالتين السابقتين لا تحرك الدعوى الجنائية إلا بناءً على شكوى من المجني عليه, أو ممثله القانوني, أو أصحاب الحقوق الأخرى في التقدم بالشكوى.

3 - حماية التوقيع الإلكتروني:

يعرف الفنيون التوقيع الإلكتروني بأنه ملف رقمي (شهادة رقمية) معترف بها تصدر عن إحدى الهيئات المختصة والمستقلة، وفي هذا الملف يتم تخزين الاسم، وبعض المعلومات المهمة الأخرى، مثل رقم التسلسل، وتاريخ انتهاء الشهادة ومصدرها، وتحتوي هذه الشهادة عند تسليمها على مفتاحين (المفتاح العام، والمفتاح الخاص)، ويعتبر المفتاح الخاص هو التوقيع الإلكتروني الذي يميز صاحبه عن بقية الناس، أما المفتاح العام فيتم نشره في الدليل وهو متاح للعامة من الناس للتعامل مع صاحبه[1].

وقد عرفه القانون رقم (1) لسنة 2006 بشأن المعاملات والتجارة الإلكترونية لدولة الإمارات العربية المتحدة بأنه: (توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذي شكل إلكتروني، وملحق أو مرتبط منطقيًا برسالة إلكترونية، وممهور بنية توثيق أو اعتماد تلك

(1) http: // safola.com/signature.chtml

كما قرر البعض أنه: (مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته).

Jonathan Rosenar Cyber Law. The law of the internet،ed Springer، 1997، p.237

كما تم تعريفه بأنه: (وحدة قصيرة من البيانات التي تحمل علاقة رياضية مع البيانات الموجودة في محتوى الوثيقة) د. عايض راشد المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، مرجع سابق، ص 91.

الرسالة).

أما القانون الفيدرالي في الولايات المتحدة الأمريكية بشأن التجارة الإلكترونية الصادر في 30 يونيو 2000،([1]) والمعمول به من أول أكتوبر من نفس العام، فيعرف التوقيع الإلكتروني بأنه (أصوات أو إشارات أو رموز أو أي إجراء آخر يتصل منطقيًا بنظام معالجة المعلومات إلكترونيًا، ويقترن بتعاقد أو مستند أو محرر، ويستخدمه الشخص قاصدًا التوقيع على المحرر).[2]

التوجيه الأوروبي رقم 1999/93، والصادر عن المجلس في 13

(1) The US Electronic Signatures in Global and National Commerce Act, E- Sign Act-(2000)

(2) دشن الرئيس الأمريكي بيل كلينتون في يونيو 2000 عصر التوقيع الإلكتروني بإجازته أول قانون أمريكي للتوقيع الإلكتروني، مستخدما اسمًا كوديا هو اسم كلبه بادي لإمضاء القانون، وبحضور مائة من رجال الأعمال وطلبة كليات الكمبيوتر في الجامعات الأمريكية، تواجدوا بقاعة الكونجرس في المنتزه القومي بفيلادلفيا، حيث أعطى الرئيس الأمريكي صيغة التوقيع عبر جهاز الكمبيوتر نفس قوة وقانونية التوقيع بالطرق التقليدية باستخدام الورقة والقلم، وعدّد كلينتون فوائد هذه التكنولوجيا الجديدة قائلا إنها ستوفر ملايين الدولارات، لأنها ستوفر أطنان الورق وملايين الوثائق التي يمكن أن تملأ المخازن، وقال عقب التوقيع: إن الإمضاء على شاشة الكمبيوتر ستكون له نفس القوة القانونية المساوية للإمضاء على الورق، ومن هنا يمكن استخدام التقنية الجديدة لتوكيل محام، أو توقيع عقد مع شركة تأمين أو رهن عقاري، أو فتح حساب بنكي، وأضاف أن القانون الجديد سيحفز التجارة الإلكترونية ويشجعها، ويعطي زخمًا للتوسع والتبادل التجاري والاقتصادي.
جريدة البيان الإماراتية، عدد 1 يوليو 2000.
http://www.albayan.co.ae/albayan/2000/07/01/ola/4.htm
والقانون موجود على الموقع:
http:/www.eg.astate.et.us/2000/rpt/oir/htm/2000،1،0795.htm

ديسمبر 1999 فقد قرر أن التوقيع الإلكتروني عبارة عن معلومات أو معطيات في شكل إلكتروني ترتبط أو تتصل منطقيًا بمعطيات إلكترونية أخرى (رسالة أو مستند) وتستخدم كوسيلة لإقرارها.

واشترط أن تتحقق الشروط التالية لصحته:

1) أن يخص صاحبه دون غيره.

2) أن يسمح بالتعرف على صاحبه.

3) أن يتم بوسائل تمكن صاحبه من الاحتفاظ به تحت سيطرته وحده دون غيره.

4) أن يتم ربطه بالبيانات التي وقع به عليها، بحيث يمكن اكتشاف أي تعديل لاحق لها.

كما أناط التوجيه بأحد مقدمي خدمات المعلومات مهمة التحقق من نسبة التوقيع إلى صاحبه.

وعرفه قانون التجارة الإلكترونية الصادر بدولة البحرين - وهي من أولى الدول العربية التي وضعت تقنينًا للتجارة الإلكترونية - بأنه: (معلومات في شكل إلكتروني تكون موجودة في سجل إلكتروني، أو مثبتة أو مقترنة به منطقيًا، ويمكن للموقِّع استعمالها لإثبات هويته).

أما القانون المصري الخاص بالتوقيع الإلكتروني فقد عرفه بأنه: (بيانات قد تتخذ هيئة حروف أو أرقام أو رموز أو إشارات أو غيرها، مدرجة بشكل إلكتروني أو رقمي أو ضوئي أو أي وسيلة أخرى مستحدثة، في رسالة بيانات أو مضافة عليها أو مرتبطة بها ارتباطًا منطقيًا وله طابع منفرد، مما يسمح بتحديد شخصية الموقِّع ويميزه عن غيره، وينسب إليه محررًا بعينه).

والملاحظ من التعريفات السابقة أنها متقاربة مع اختلاف الألفاظ، أما

المضمون فهو واحد، ونستطيع القول بأن التوقيع الإلكتروني ما هو إلا مجموعة من الرموز أو الأرقام أو الحروف الإلكترونية التي تدل على شخصية الموقّع دون غيره[1].

أو كما قرر بعض الفقه بأنه: كل إشارات أو رموز أو حروف مرخص بها من الجهة المختصة باعتماد التوقيع ومرتبطة ارتباطًا وثيقًا بالتصرف القانوني، تسمح بتمييز شخص صاحبها وتحديد هويته، وتنم دون غموض عن رضائه بهذا التصرف القانوني[2].

والتوقيع الإلكتروني شأنه شأن أي اختراع جديد، فبجانب إيجابياته المتعددة والتي سهلت الكثير من العمليات سواء على المستوى التجاري أو الشخصي، إلا أنه يظل محفوفًا بالمخاطر، وقد يثير عدة مشكلات عملية وقانونية لدى استخدامه.

ومن أهم المشكلات التي قد تثار عند استخدام التوقيع الإلكتروني التحايل، سواء من صاحب التوقيع مرسل الرسالة، أو مستقبلها، أو من الغير، فقد يكون الشخص الذي يضع توقيعه على المحرر ليس هو ذات الشخص صاحب هذا التوقيع، أو قد يستخدم المستفيد من التوقيع على المحرر هذا التوقيع لأكثر من مرة متجاوزًا قصد صاحبه الذي وضعه، ويحاول القائمون على التكنولوجيا تطويرها للحد من إساءة استخدام التوقيع الإلكتروني.

وتعد مشكلة تزوير التوقيع الإلكتروني من الجرائم المطروحة وبقوة على الساحة، وخصوصًا مع تزايد حالات الاحتيال والتسلل غير المشروع

(1) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، 2004، ص 10.

(2) د. ثروت عبد الحميد، التوقيع الإلكتروني، مرجع سابق، ص 50.

إلى أجهزة الحاسب الآلي عن طريق شبكة الإنترنت، والوصول إلى الشفرة الخاصة بصاحب التوقيع الإلكتروني، ثم القيام بنسخها أو تزويرها، ووضعها على محرر مزور واستخدام هذا المحرر.

ويقصد بالتزوير المعلوماتي والذي سنتكلم عنه تفصيلا لاحقًا (أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي، سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة، أو كانت مرسومة عن طريق الراسم، ويستوي في المحرر المعلوماتي أن يكون مدونًا باللغة العربية أو لغة أخرى لها دلالتها, كذلك قد يتم في مخرجات غير ورقية شرط أن تكون محفوظة على دعامة - كبرنامج منسوخ على أسطوانة - وبشرط أن يكون المحرر المعلوماتي ذا أثر في إثبات حق أو أثر قانوني معين[1], كما نعتقد بإمكانية حدوث التزوير على البيانات المخزنة داخل النظام دون استخراجها).

ومن أشهر الوسائل التي يمكن الاعتماد عليها في تقليد أو تزوير التوقيع الإلكتروني استخدام برامج حاسوبية وأنظمة معلوماتية خاصة بذلك الأمر، يتم تصميمها على غرار البرامج والأنظمة المشروعة، أو محاولة البعض كسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها وإعادة استخدامها بعد ذلك[2].

ومن الجرائم الأخرى والتي تمس التوقيع الإلكتروني جريمة الدخول غير المشروع إلى أنظمة المعلومات أو قاعدة البيانات المتعلقة بالتوقيع

---

(1) عبد الفتاح بيومي حجازي - الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت - الطبعة الاول دار الكتب القانونية، المحلة الكبرى، 2001, ص 170.

(2) د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, دار النهضة العربية, 2009, ص 242.

الإلكتروني, وما يتبع ذلك من أفعال غير مشروعة, وسوف نتناول الجرائم الواقعة على التوقيع الإلكتروني بشيء من التفصيل في الباب الثاني.

كما قد يتعارض التوقيع الإلكتروني مع بعض القوانين القائمة، ومنها على سبيل المثال قانون الإثبات، فمفهوم التوقيع فيه لا يكون إلا على مستند ورقي، وبصورة محددة في القانون على سبيل الحصر، وبالتالي لا نستطيع القول بانطباق ذلك على التوقيع الإلكتروني.

كما أن قانون الإثبات مثله في ذلك مثل أغلب القوانين القائمة لا يستطيع مسايرة السرعة الناتجة عن معالجة المعلومات إلكترونيًا، فلا شك أن إدخال الحاسب الإلكتروني في مجال معالجة المعلومات يؤدي إلى سرعة إنجاز هذه المعلومات، خصوصًا في ظل تعدد الإجراءات الواجبة بل وتكرارها، ويبدو التوقيع التقليدي في ظل هذه السرعة عقبة تعرقل سير الإجراءات بالسرعة اللازمة[1].

والمشرع الفرنسي اهتم بموضوع التوقيع الإلكتروني في القانون رقم 230 لعام 2000 والمتعلق بالحق في الإثبات وتكنولوجيا المعلومات والتوقيع الإلكتروني، حيث نص صراحة في المادة 1/1316 على المساواة التامة في الحجية كدليل في الإثبات بين الكتابة الإلكترونية والكتابة على الورق.

وإن كان المشرع قد أعقب ذلك بالنص في المادة نفسها على أنه يشترط أن تكون هذه الكتابة الإلكترونية تعبر عن الشخص الذي صدرت عنه قانونًا، ولم يكتف المشرع الفرنسي بهذا النص الصريح في المساواة بين الكتابتين، بل أعقبه بنص أكثر حسمًا وهو نص المادة (3/1316) والتي قررت أن الكتابة على محتوى إلكتروني لها نفس القوة في الإثبات كالكتابة

(1) د. السيد عتيق، جرائم الإنترنت، مرجع سابق، ص 114.

على محتوى ورقي.[1]

وبذلك يكون المشرع الفرنسي قد نص صراحة على القيمة القانونية للمستند الإلكتروني في الإثبات بلا أي تفرقة بينه وبين مثيله الورقي، وهو بذلك يكون قد حسم خلافًا في الفقه استمر سنوات، وبالتالي يجرم الاعتداء على هذا التوقيع الإلكتروني، شأنه في ذلك شأن التوقيع التقليدي.[2]

كما قام المشرع بدولة الإمارات العربية المتحدة بتعديل قانون الإثبات بالقانون الاتحادي رقم (36) لسنة 2006، وذلك بتعديل بعض أحكام قانون الإثبات في المعاملات المدنية والتجارية الصادر بالقانون الاتحادي رقم (10) لسنة 1992 بإضافة بند جديد برقم (3) إلى المادة (17) من قانون الإثبات في المعاملات المدنية والتجارية المشار إليه يكون نصه الآتي: (يكون الوفاء عن طريق الوسائط الإلكترونية مبرئًا للذمة، وذلك وفق ما يحدده وزير العدل بالتنسيق مع الجهات المعنية).

كما أضاف فصلا جديدًا إلى الباب الثاني بعنوان (الفصل الثاني مكرر) وأضاف فيه مادة جديدة برقم (17) مكرر نصها الآتي:

1) يعتبر توقيعًا إلكترونيًا كل أحرف أو أرقام أو رموز أو إشارات أو صور أو أصوات لها طابع منفرد تسمح بتحديد شخص صاحب التوقيع وتمييزه عن غيره على النحو الوارد في قانون المعاملات والتجارة الإلكترونية..

---

(1) د. فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، رسالة دكتوراه مقدمة إلى أكاديمية الشرطة، مصر، 2007، ص 102.

(2) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 23.

2) يعتبر محررًا إلكترونيًا كل انتقال أو إرسال أو استقبال أو تخزين لرموز أو إشارات أو كتابة أو صور أو أصوات أو معلومات أيًا كانت طبيعتها تجري من خلال وسيلة تقنية معلومات.

3) للتوقيع الإلكتروني ذات الحجية المقررة للتوقيعات المشار إليها في هذا القانون إذا روعي فيه الأحكام المقررة في قانون المعاملات والتجارة الإلكترونية.

4) للكتابة الإلكترونية والمحررات الإلكترونية والسجلات والمستندات الإلكترونية ذات الحجة المقررة للكتابة والمحررات الرسمية والعرفية في أحكام هذا القانون متى استوفت الشروط والأحكام المقررة في قانون المعاملات والتجارة الإلكترونية.

ولتوفير حماية فعالة للتوقيع الإلكتروني وحفاظًا على المصالح المالية لأطراف التجارة الإلكترونية، فقد تدخلت التشريعات في العديد من الدول لتقرير حماية جنائية للتوقيع الإلكتروني، ووضعت نصوصًا عقابية لجرائم إتلاف أو تزوير توقيع أو محرر إلكتروني، واغتصاب التوقيع الإلكتروني، واستعمال توقيع أو محرر مزور، وإنشاء أو استعمال توقيع إلكتروني لغرض احتيالي، وتحريف أو تغيير أو استعمال أداة إنشاء توقيع إلكتروني، ونسخ أو حيازة أداة إنشاء توقيع إلكتروني، وجريمة انتهاك سرية بيانات التوقيع الإلكتروني أو أداة إنشائه، وغيرها من الجرائم التي تمثل اعتداءً على التوقيع الإلكتروني.

4 - حماية المستهلك من الغش والتحايل:

حماية المستهلك الإلكتروني من الغش والتحايل مصلحة مهمة يحميها القانون، وهي حق للمستهلك الذي يتعامل عبر شبكة الإنترنت، شأنه في ذلك شأن المستهلك العادي، مع الأخذ في الاعتبار التقنية الفنية المستخدمة في

التعامل، وقد اهتم مشروع قانون التجارة الإلكترونية المصري الحالي بحماية المستهلك، وأفرد له بابًا مستقلا هو الباب التاسع منه، ونص فيه على عدة مبادئ لتغطية مفهوم حماية المستهلك[1].

كما نص القانون التونسي الخاص بالتجارة الإلكترونية في الباب الخامس منه على حق المستهلك في الحماية بضرورة أن يوفر له البائع البيانات الجوهرية وشروط التعاقد وطريقة الشحن، وهذه المعلومات يجب توافرها إلكترونيًا، كما نص القانون على أن عملية الدفع الإلكتروني تخضع للتشريع الساري.

وتوصلت دراسة أجرتها إحدى جمعيات المستهلكين في أمريكا إلى أن شركات عدة جمعت معلومات شخصية جدًا وغير ضرورية عن المستهلكين، وقالت هذه الجمعية: إن احترام الحياة الشخصية حق معترف به كحق أساسي من حقوق الإنسان، لكن مع ذلك اكتشفنا أن كثيرًا من الشركات جمعت كمًّا وافرًا من المعلومات الشخصية جدًا وغير الضرورية بخصوص المستهلكين، وأكدت أن ثلثي المواقع الأمريكية التي شملتها الدراسة ما زالت تطلب من مستخدمي الشبكة تزويدها بمعلومات شخصية، ثم تقوم بعد ذلك باستخدام هذه المعلومات كما هي أو خارج إطارها.[2]

وتحاول أغلب قوانين حماية المستهلك تأمين أقصى درجات الحماية الجنائية للمستهلك, كما اهتمت بعض القوانين بصورة خاصة بالمستهلك الإلكتروني وأفردت له نصوصًا خاصة, ومن الجرائم التي عاقبت عليها

(1) د. ميرفت عبد المنعم الصادق، الحماية الجنائية للمستهلك، مرجع سابق، ص 249 وما بعدها.
(2) http://www.middle.east.online.com/Tech/jan2001/internet privacy 2/2/2001 htm.

القوانين جريمة عدم التنبيه إلى خطورة استعمال السلعة أو الخدمة[1], كما خولت بعض القوانين للمستهلك حق الرجوع عن العقد خلال مدد محددة إذا وجد هناك ما يضر بمركزه القانوني.

5 - حماية أسماء الحقول **Domain Name** وحقوق الملكية الفكرية:

نتيجة لتطور شبكة الإنترنت نشأت مشكلة عندما ارتفع عدد أجهزة الكمبيوتر المضيفة فزاد عن ألفي جهاز، وكان يجب أن يخصص اسم لكل كمبيوتر مضيف، وسعيًا لحل هذه المشكلة، تم طرح نظام اسم النطاق في نوفمبر 1983، وهو يشبه في تكوينه شجرة متفرعة، وفيه يخصص لكل عنوان هيكل هرمي، وبعد بعض المناقشات تم تطبيق مخطط لوضع العناوين من خاص إلى عام، وفي نهاية الأمر تم الاتفاق على سبعة نطاقات رئيسية وهي edu وcom وgov وmil وnet وorg وint. وبدأت شبكة ARPA تتطلب تطبيق نظام اسم النطاق في عام 1985، حتى أصبح نظام اسم النطاق مقبولا على المستوى العام في عام 1986.

ولقد تأسست هيئة الإنترنت المعنية بالأرقام المخصصة IANA بصورة غير رسمية، وتحكمت في تخصيص عناوين بروتوكولات الإنترنت، وإدارة المناطق الجذرية لنظام اسم النطاق، فضلا عن مهام أخرى تتعلق ببروتوكول الإنترنت.

---

(1) تنص المادة (18) من القانون الاتحادي رقم 24 لسنة 2006 في شأن حماية المستهلك على أنه: (مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر, يعاقب بالغرامة التي لا تقل عن ألف درهم كل من يخالف أحكام هذا القانون والقرارات الصادرة تنفيذًا له, وإذا لم ينبه المزود إلى خطورة استعمال السلعة أو الخدمة بشكل ظاهر ونتج عن ذلك ضرر كانت العقوبة الغرامة التي لا تقل عن عشرة آلاف درهم).

وفي عام 1998 تم إعادة تنظيم هيئة الإنترنت المعنية بالأرقام المخصصة IANA ومركز شبكة معلومات الإنترنت InterNIC باسم مؤسسة تحديد الأسماء والأرقام عبر الإنترنت (إيكان ICAN).

وفي 24 ديسمبر 1998 أبرمت جامعة جنوب كاليفورنيا اتفاقًا مع مؤسسة إيكان، لتحويل وظائف هيئة الإنترنت المعنية بالأرقام المخصصة إلى مؤسسة إيكان، بحيث يبدأ سريان هذا الاتفاق اعتبارًا من 1 يناير 1999.

ومواقع الإنترنت لها أهمية كبيرة في الشبكة المعلوماتية، وللوصول إلى هذه المواقع كان يتعين إيجاد آلية معينة تمتاز بالسهولة واليسر وتمثل حلقة وصل بين المستخدم والموقع المراد الوصول إليه, فظهرت في البداية فكرة الأرقام الممثلة لعنوان موقع ما, ونظرًا لما واجهته من صعوبة في حفظها نظرًا لطول هذه الأرقام وتعقدها, ظهرت فكرة أخرى وهي تحويل هذه الأرقام إلى أحرف تتم كتابتها بطريقة معينة تؤدي للوصول إلى الموقع المطلوب[1].

وفقًا للتعريف الذي ورد في مشروع قانون التجارة الإلكترونية المصري يقصد باسم الدومين: عنوان منفرد للمواقع الموجودة على شبكة الإنترنت تسمح بتحديد الموقع وتمييزه عن غيره.[2]

(1) يعد العنوان symbplics.com هو أول عنوان إلكتروني تم تسجيله.
Real - life Corpoate Domain Name challenges, Issues and strategic Solution Available at: www.verisign.com

(2) ما هو الدومين نيم domain name ؟ كما أن لكل مكان بالحياة عنوانًا فللمواقع على شبكة الإنترنت أيضا عنوان، عندما تريد أن يزورك شخص ما فإنك تعطيه عنوانك الذي يستطيع الذهاب إليه حتى يستطيع مقابلتك، فكذلك لمواقع شبكة الإنترنت وصف للوصول، ويطلق عليها domain name اسم النطاق أو اسم الاختصاص،=

وتعرف أسماء الحقول بأنها ترجمة لأرقام تتم عن طريق حروف معينة تسمح بدوران المعلومات عبر شبكة الإنترنت, كما عرفت بأنها مجرد تحويل أو نقل مجموعة من الأرقام في صورة حروف تشكل مصطلحًا تتناسب مع اسم المشروع أو المنظمة[1].

كما عرف بأنه اسم ينفرد به حائزه عبر الإنترنت، فهو جزء من (URL)[2] الذي يتعامل مع الخادم ويقوم بتتبع طلب الصفحة أو الموقع, ومن حيث الشكل فهو سلسلة من الكلمات يفصل بينها نقاط تتولى تعريف

= وهذا الاسم يكون بصورة عامة على الشكل التالي:
DOMAIN.COM, عـــلى ســـبيل المثـــال MIXXAT.COM أوWWW.MIXXAT.COM
و هو يتكون من جزأين، فالجزء الأول كما بالمثال domain name ويوضع بدلا منه اسم الموقع أو اختصار له أو ما يراه صاحب الموقع كاسم عام له، ثم توضع علامة النقطة (الدوتDot). .ثم يلي ذلك نوع النطاق، وهو غالبًا ما يكون بحسب نشاط الموقع أو أهدافه..وأنواع النطاق تختلف باختلاف الموقع، ومن أشهرها:
com وnet وorg وهناك أنواع أخرى كثيرة مثل ws أو info أوbiz وتختلف باختلاف المعنى الذي تدل عليه..فنوع النطاق com اختصار ل commercial وتشير إلى تجاري، ونوع النطاق net اختصار لـ networkوتشير إلى شبكة، ونوع النطاق org اختصار لـ organization وتشير إلى خيري أو منظمة غير ربحية، ونوع النطاق ws اختصار لـ site****** وتشير إلى موقع، ويقال: إنه اختصار لاسم مدينة من المدن، ونوع النطاق info اختصار لـ information وتشير إلى معلوماتية، ونوع النطاق biz اختصار لـbusiness وتشير إلى التجارة، راجع حول ذلك:http://vb.mixxat.com/t9878.html

(1) Richard Milchir (M), Marques et Noms De domain de quelques Problemes Actuels.lamy droit commercial. No 135. juillet. 2000. Bulletin d'actualite. P.2.

(2) Uniform Resource Locater

عنوان بروتوكول الإنترنت[1].

والترجمة الحقيقية أنه اسم الحقل Domain Name كما ترجم في القانون النموذجي للأمم المتحدة المتعلق بالتجارة الإلكترونية، وإن كان في الترجمة الحرفية يمكن أن نطلق عليه تعبير اسم المجال أو اسم النفوذ أو اسم النطاق تعبيرًا عن أحقية شخص ما بهذا الاسم، والبعض الآخر يفضل تسميته باسم الدومين كما اشتهر عنه، والأهم من ذلك أنه يعتبر دليلا لمستخدمي شبكة الإنترنت، فمثلا مكان منظمة التجارة العالمية على الشبكة هو http://www.wto.org والحروفWWW تشير إلى الشبكة الشاملة للعالم أي المقصود بها شبكة الإنترنت، واسم الدومين يجب أن يكون على الأقل من جزئين؛ الجزء الأول وهو المستوى الأعلى للاسم الدومين وهو " tell top- level domain name"D وفي المثال الذي عرضناه يمثل كلمة منظمة ORG (ORGANIZATIAN) والجزء الثاني يعرف بأنه المستوى الثاني لاسم الدومين، وهو في مثالنا " W T O " أي World trade organization ويعني منظمة التجارة العالمية، ويضاف إلى ذلك رقم دولي لتحديد المكان ونوع المكان واسم المتواجد فيه على الشبكة لاستيفاء طلبات المتعاملين في مجال التجارة الإلكترونية[2].

واسم الدومين يتشابه في ذلك مع العلامة التجارية للإعلان عن السلعة، كوسيلة تشير إلى وجود السلعة أو الخدمة على شبكة الإنترنت، ومع تزايد التعامل على شبكة الإنترنت ستتزايد أسماء الدومين، ويمكن أن تتضارب مع العلامات التجارية، وهو ما تقتضي المصلحة الواجب حمايتها تنظيم

(1) د. عمر محمد أبو بكر بن يونس، الإيكان، دار النهضة العربية، 2005، ص 29.
(2) د. وليد عودة، الموسوعة الحاسوبية، الإصدار الأول،2003، ص 356.

تسجيل الاثنين معًا.[1]

ولتنظيم أسماء الدومين ظهرت هيئة شبكة الإنترنت للأسماء والأرقام المخصصة (الآيكان) ICAN وهي منظمة غير ربحية تم تأسيسها دوليًا لتتولى مسئولية توزيع مجالات العناوين في بروتوكول شبكة الإنترنت، وتخصيص معرَفات البروتوكول، وإدارة نظام سجلات المواقع العامة عالية المستوى (gTLD) وسجلات المواقع عالية المستوى لرمز الدولة (ccTLD)، كما أنها تضطلع بمسئولية وظائف إدارة نظام الخوادم المركزية، وقد كانت هذه الخدمات تقدم أصلا بموجب عقد حكومي أمريكي، من قِبَل سلطة تخصيص أسماء شبكة الإنترنت (IANA) وغيرها من الهيئات، أما الآن فتقوم الآيكان بالمهام التي كانت تؤديها هذه السلطة.

ونظرًا لكونها شراكة بين القطاعين العام والخاص، تلتزم الآيكان بالمحافظة على الاستقرار التشغيلي لشبكة الإنترنت، وتعزيز روح المنافسة، وتحقيق تمثيل واسع النطاق لمجتمعات شبكة الإنترنت العالمية، إضافة إلى سعيها لصياغة سياسات تلائم رسالتها من خلال عمليات تعتمد على استطلاع الآراء من القاعدة إلى القمة مرورًا بجميع المستويات.[2]

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 25.

(2) يساعد نظام أسماء المواقع (DNS) مستخدمي شبكة الإنترنت في الوصول إلى ما يبحثون عنه في رحاب شبكة الإنترنت، حيث يوجد لكل جهاز حاسوب متصل بالإنترنت عنوان مستقل يسمى "عنوان بروتوكول شبكة الإنترنت (IP Address)". ونظرًا لصعوبة تذكر عناوين بروتوكول شبكة الإنترنت (حيث إنها عبارة عن سلاسل من الأرقام)، فقد استبدل بنظام هذه الأرقام كأسماء للمواقع مجموعات من الحروف المألوفة (التي تشكل "أسماء المواقع"). فعوضًا عن كتابة الرقم: "192.0.34.65"، يمكنك كتابة اسم مثل www.icann.org. =

وتتولى الآيكان مسئولية تنسيق إدارة العناصر الفنية في نظام أسماء المواقع، وذلك لضمان تيسير الاتصال بالمواقع على نطاق العالم، بحيث يتسنى لجميع مستخدمي شبكة الإنترنت إيجاد العناوين الصحيحة، وتقوم الآيكان بهذا عن طريق مراقبة توزيع المعرفات الفنية المستخدمة في عمليات شبكة الإنترنت، وتخصيص أسماء المواقع العليا (ومثال ذلك info،com.، وغيرها).

وسوف نتناول لاحقًا الاعتداء على نطاق أسماء الحقول (الدومين نيم) عند حديثنا عن الجرائم الواقعة على بيانات التجارة الإلكترونية من ناحية، وعن الاعتداء على العلامات التجارية من ناحية أخرى.

= ويقوم نظام أسماء المواقع بترجمة الاسم الذي تكتبه إلى عنوان بروتوكول شبكة الإنترنت المقابل، ثم يوصلك بالموقع الإلكتروني الذي ترغب في زيارته، كما يساعد نظام أسماء المواقع على تشغيل البريد الإلكتروني بالشكل الصحيح بحيث تصل رسالتك إلى المرسل إليه المقصود.
وقد أوجدت الآيكان سوقًا تنافسية لتسجيلات أسماء المواقع العامة عالية المستوى، مما أدى إلى تخفيض تكاليف أسماء المواقع بنسبة 80%، مما وفر على المستهلكين والشركات والأعمال ما يزيد عن مليار دولار أمريكي سنويًا من رسوم تسجيل المواقع.
كما قامت الآيكان بتنفيذ السياسة الموحدة لحل نزاعات أسماء المواقع (UDRP) حيث تم استخدامها لحل أكثر من 5000 نزاع على حقوق أسماء المواقع، وقد صممت هذه السياسة لتكون فاعلة ومنخفضة التكلفة.
وبالتنسيق مع المجتمعات الفنية وأصحاب المصالح المناسبين، اعتمدت الآيكان إرشادات خاصة بنشر أسماء المواقع الدولية (IDN)، مما أتاح الفرصة لتسجيل مواقع بمئات اللغات حول العالم. للمزيد حول الآيكان الاطلاع على الموقع:

http://www.icann.org/tr/arabic.html

المطلب الثاني

الحماية الجنائية لأطراف عقود التجارة الإلكترونية

يتطلب قيام التجارة الإلكترونية من التاجر أو الشركة إنشاء موقع على الشبكة الدولية للمعلومات " شبكة الإنترنت "، بهدف الإعلان عن السلع التي يقوم بإنتاجها أو تسويقها، أو الخدمات التي يود عرضها على الجمهور في كل أنحاء العالم، ويفترض أن مواقع التجارة الإلكترونية تحتوي من خلال صفحاتها على مجموعة بيانات أو معطيات خاصة بالمنتج أو موزع السلعة أو الخدمات، وصور وأشكال ثابتة أو متحركة للدعاية أو لتحديد مواصفات السلعة أو الخدمة، كما تخصص هذه المواقع جزءًا لتبادل المعلومات الخاصة بالعميل، وهي عادة بيانات خاصة باسمه وعنوانه ورقم بطاقته الائتمانية والتي يستخدمها في السداد، ثم طريقة تسليم السلعة أو الخدمة.

كما أن هناك مجموعة من المشكلات الفنية والتقنية المتعلقة بحماية مواقع شبكة الإنترنت من الاختراق والتعديل والتبديل والإتلاف، وهي مشكلات تتعلق بالمتخصصين في مجال تصميم مواقع شبكة الإنترنت وبرمجة الكمبيوتر والتشفير[1]، فإن هناك مشكلات قانونية مرتبطة بحماية موقع التجارة الإلكترونية، والذي يعتبر المكان المناسب لإتاحة المعلومات على شبكة الإنترنت من خلال عنوان محدد، وبالتالي وجب حمايته من الدخول غير المشروع أو البقاء فيه؛ لأن ذلك قد يؤدي إلى تعديل أو إتلاف

(1) كثر مؤخرًا عدد الشركات المتخصصة في مجال المعلوماتية والبرمجة وتصميم وسائل الآمان لمواقع التجارة الإلكترونية، وحمايتها من السطو الإلكتروني، والولوج والنصب المعلوماتي، وبالأخص في الولايات المتحدة الأمريكية وأوروبا.

للبيانات الواردة في هـذا الموقـع.

وبما أن الموقـع الإلكتروني يعتـبر أحـد الـنظم المعلوماتيـة الجـديرة بالحمايـة، فـإن نصـوص حماية نظام المعالجة الآلية للمعلومات تنطبق عليه، وهـذه النـصوص جاءت في صورة تشريعات حديثة تممت نصوص القوانين العقابية التي كانت عاجزة عـن مواجهـة الجـرائم الماسـة بـنظم المعالجـة الآليـة للمعلومات، وإذا كانت أغلب التشريعات العقابية العربية لم تلحق بهذا الركـب باستثناء دول قليلة جدًا، فإن التشريعات الجنائيـة المقارنـة فطنـت إلى ضـرورة حمايـة الـنظم المعلوماتيـة مـن جـرائم القرصـنة، والتـي أصـبحت العـائق الأول أمـام نمـو قطـاع التجـارة الإلكترونية[1].

ولما كان موقع التجارة الإلكترونية في حاجة إلى حماية جنائية في مواجهة جرائم الاختراق أو الدخول غير المشروع، وبالتالي حمايـة التاجر صاحب هذا الموقع، فإن العميل المستهلك في حاجـة أيضًا إلى حماية جنائية وعلى الخصـوص في مجـال عقـود التجـارة الإلكترونيـة، وفي الحـديث عـن حماية أطراف عقود التجارة الإلكترونية لابـد أن نتطرق لمسألة حمايـة الموقـع الإلكـتروني للتـاجر على شبكة الإنترنت في الفرع الأول، ثم الحماية الجنائية للمستهلك في الفرع الثاني.

الفرع الأول

حماية مقر التاجر الإلكتروني

اهتمت التشريعات بالولايات المتحـدة الأمريكيـة وأوروبا في العقود الأخيرة بمسـألة حمايـة مواقـع شبكة الإنترنت بصفة عامة ومواقع التجارة

(1) Daniel Martin: La menace de la cybercriminalite, Revue des problemes economiques, n 2706, 28mars2001, p19

الإلكترونية على وجه الخصوص، ويظهر ذلك من خلال مجموعة من القوانين التي تستهدف تجريم صور الاعتداء على أجهزة الحاسب وبرامجها وقواعد البيانات، والملاحظ أن الاعتداء على مواقع شبكة الإنترنت وصفحاتها بما تتضمنه من معلومات يعتبر صورة من صور الاعتداء على النظم المعلوماتية، نظرًا لأن إعداد مواقع التجارة الإلكترونية يتطلب بالضرورة استخدام أجهزة كمبيوتر وبرامج مختلفة، ثم إن جرائم الدخول غير المشروع لمواقع التجارة الإلكترونية يصنف ضمن جرائم التعدي على نظم المعالجة الآلية للبيانات، فنظام التجارة الإلكترونية كأي نظام معلوماتي يستند إلى قاعدة بيانات[1]، ثم إن تجريم الدخول غير المشروع أو البقاء غير المشروع داخل الموقع هو البوابة الأولى لحماية هذا النظام[2].

فالتجارة الإلكترونية في حاجة إلى ثقة كل الأطراف المتعاملين بها سواء أكانوا منتجين أو تجارًا، أو مستهلكين، وذلك يتحقق من خلال اتخاذ إجراءات قانونية ضد من يعتدي على نظم البيانات المتعلقة بهذه التجارة، وقد تتعرض مقار الشركات أو التجار على شبكة الإنترنت لأنواع متعددة من المخاطر تتناسب مع حجم المقر المعلوماتي، وأسلوب بنائه، والمكان الذي يبث منه المعلومات، وارتباط ذلك بالنظم الداخلية للشركة، والتي دائمًا ما يكون مصدرها مجرم شبكة الإنترنت (الهاكر).[3]

---

(1) Nicole Tortello et Pascal Lointier: Internet pour les jurists, Dalloz, 1996, p23

(2) رأفت رضوان، عالم التجارة الإلكترونية، مرجع سابق، ص103

(3) الهاكرز هو شخص خبير بلغة البرمجة يقوم بالدخول على غيره والتجسس عليهم، وأول ما ظهر في عام 1984 عندما استطاع ليكس لوثر إنشاء مجموعة من القراصنة يقومون بالدخول على أجهزة الآخرين، ثم ظهرت عام 1990 مجموعة =

ومعناه " المجرم التقني " وهو مجرم سلك سبيل التقنية لارتكاب جرائمه، والمتمثل في استخدامه لتقنية المعلومات هنا، ويطلق عليه أيضًا مصطلح "المجرم المعلوماتي" وإن كانت التسمية الحقيقية له هي **"مجرم شبكة الإنترنت"** أو **"هاكر"** وجمعها **"هكرة"**.

= أخرى قامت بمنافستهم وحاول كل طرف اختراق الآخر حتى سميت حرب الهاكرز العظمى، واستمرت أربع سنوات انتهت بإلقاء القبض على بعضهم، ويعتبر كيفن ميتنيك أشهر هاكر في التاريخ استطاع اختراق كمبيوتر الشركة التي يعمل بها، وحبس لمدة عام، وخرج أكثر ذكاء ومارس هوايته، وكانت أكبر قضاياه سرقة أرقام 2000 بطاقة ائتمان.

- راجع حول ذلك: د. ممدوح عبد الحميد، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، الشارقة، 2001، ص 158.

ويعود الفضل في الكشف عن مصطلح الهكترة Hacking إلى كاتب الخيال العلمي الكندي/ الأمريكي وليم جيبسون W. Jibson في مؤلفه،The New Romancer الذي أصدره عام 1984، ولقد لقي هذا المؤلف نجاحًا كبيرًا في إطار استخدام هذا المصطلح، لاسيما حين تشخيصه في المجرم التقني أو مجرم شبكة الإنترنت (هاكر) Hacker الذي كان آنذاك ذا شمولية أكثر بحيث احتوى كافة أشكال الإجرام عبر شبكة الإنترنت, والجدير بالذكر إن مصطلح هاكر قبل عام (1984) لم يكن يشير إلى الإجرام، فقد أطلق هذا المصطلح على أشخاص يملكون قدرات تقنية عالية المستوى كما أسلفنا، إذ أطلق على المبرمجين المبدعين في معهد ماساشوستس للتكنولوجيا، وعلى مبرمجي جامعة Stanford وجامعة Berkeley في الولايات المتحدة الأمريكية لكونهم برعوا في الحركة عبر شبكة الإنترنت, واليوم يشير المصطلح - وبعد تطويره إلى Cracker (أحد نماذج الهاكر سيئ النية) - إلى الأنشطة الإجرامية المتعلقة بجرائم شبكة الإنترنت، وأحيانا كما يشار لهم (منذ العام 1995) مثلما اقترح الأستاذان هافنر وماركوف HAFNER & MARKOFF بـ... تافهي العالم الافتراضي punks،Cyber .

- د. عمر محمد بن يونس، ورقة عمل بعنوان: مجرم شبكة الإنترنت (محاولة تأريخ لعلم الإجرام عبر شبكة الإنترنت)، ص 2.

ويرتبط سلوك أو نشاط مجرم شبكة الإنترنت بظاهرة الاختراق Intrusion وهم يتمتعـون بمهارات خاصة، وكثيراً ما يطلق على سادة الاختـراق مصـطلح **"قراصـنة شـبكة الإنترنـت"**، وهـذا المصطلح الأخير لا يتعلق بالاختراق تحديدًا وإنما بموضوع آخر وهو العدوان على حقـوق الملكيـة الفكرية تحديدًا.[1]

وسوف نستعرض هذه المخاطر التي تواجه المقر ومستويات تـأمين هـذا المقـر عـلى النحـو الآتي:

أولا: المخاطر التي تواجه مقر الشركة:

- **تغيير محتوى المقر:**

ويتم ذلك بالتأثير عـلى شـكل المقـر بمـا يجعلـه مـدعاة للاسـتخفاف، وكـذلك بتغيـير بعـض المعلومات به بما يسيء إلى الشركة، أو بما يؤدي إلى إساءة العلاقة بين الشركة وعملائها، وهي أحد المخاطر المعتادة التي تتعرض لها كافة المقار بغض النظـر عـن حجـم مقـر المعلومـات، أو مكـان بـث معلومات

---

(1) في إطار جرائم شبكة الإنترنت خاصة يجب أن نميز بين مجرم شبكة الإنترنت ذاته وبين مجرم آخر يتحد معه في النشاط الإجرامي، ونقصد به مجرم الحاسوب، وذلك مـن حيـث كـونهما معـا يشـكلان المجـرم التقنـي ككل، فمجرم شبكة الإنترنت المتميـز هـو الهـاكر Hacker الـذي يتخـذ الشـكل الخبيـث لـه في مصـطلح Cracker في حين إن مجرم الحاسوب هو القرصان Pirate مرتكب جرائم العـدوان عـلى حقـوق الملكيـة الفكرية عامـة، مـع تخصـيص جزئيـة منهـا تتعلـق بمـدى إمكانياتـه التقنيـة في السـيطرة عـلى اسـتخدام الحاسوب، كما هو الشأن في اختراق كلمات العبور لملفات مشفرة مخزنة في الحاسوب، كـل ذلـك دون أن يكون الحاسوب مرتبطاً بالإنترنت تحديدًا.

- د. عمر محمد بن يونس، ورقة عمل بعنوان: مجـرم شـبكة الإنترنـت (محاولـة تـأريخ لعلـم الإجـرام عـبر شبكة الإنترنت)، مرجع سابق، ص 2.

المقر، أو ارتباط المقر بالنظم الداخلية، ويتم تغيير المحتوى هنا من خلال نوعين من الهجمات هما:

- **هجمات الهواة:** ويتم فيها تغيير لبعض المحتوى الذي يؤثر على شكل المقر ويجعل منه مدعاة للسخرية والاستخفاف، وقد تعرض مقر البيت الأبيض ومقر قيادة القوات الجوية الأمريكية لمثل هذا النوع من الهجوم، حيث تم تغيير بعض الصور المهمة بصور جنسية فاضحة حتى اضطر مديرو هذه المقار إلى غلقها لعدة أيام.

- **هجمات المحترفين:** ويقصد بها الهجمات التي تتم عن قصد من بعض الشركات المنافسة والتي تعمد إلى تغيير بعض المعلومات بالمقر بما يسئ إلى الشركة أو بما يؤدي إلى إساءة العلاقة بين الشركة وعملائها نتيجة المعلومات التي تم تعديلها بمعرفة المهاجمين.[1]

- **إغلاق المقر أمام المتصفحين[2]:**

---

(1) خالد بن نواف الحربي، الأمن والحماية في شبكة الإنترنت للمستخدم العربي، ص 10، منشور على شبكة الإنترنت: http://www.boosla.com/

(2) من أشهر الحوادث التي تعرضت لها المقار في هذا المجال ما تعرضت له شركة أمريكا أون لاين (وهي من أكبر مقدمي خدمة شبكة الإنترنت في العالم) حيث توقف نظام البريد الإلكتروني لمدة 19 ساعة في عام 1996 وأثر ذلك على عملاء الشركة بصورة مباشرة، اضطرت معها الشركة إلى انتهاج سياسة وجود احتياطي كامل لنظام البريد الإلكتروني لكل مستخدم بنسبة 100% بما يقلل من مخاطر التعرض لهذا النوع من الهجوم، وأيضا تعرض مقر البيت الأبيض لهجمة من هذا النوع أثناء ضربات الناتو ضد يوغوسلافيا وذلك بعد ضرب السفارة الصينية بصواريخ طائرات الناتو، فقام الآلاف من الصينيين بتنفيذ هجوم على مقر معلومات البيت الأبيض من خلال إرسال ملايين الرسائل التي أدت إلى توقف مقر المعلومات عن تقديم الخدمة، ومن أشهرهم الهاكر المسمى بالقاتل الإلكتروني E,Killer الذي رد على هذا القصف برد ثأري إجرامي على درجة =

= عالية من الخطورة، إذ قام القاتل الإلكتروني مع آخرين من بني جلدته بتخريب موقع صفحة السفارة

وهو من المخاطر العامة التي يمكن أن يتعرض لها أي مقر، وفيها يقوم المهاجم بشغل حاسب المقر الرئيسي Server بسيل من الرسائل والاستفسارات التي تؤدي في النهاية إلى عدم قدرة المقر على تلبية أي طلبات من مستهلكين فعليين، أو عدم قدرة أي مستهلك على الدخول إلى مقر المعلومات من الأصل، أو إبطاء ردود المقر على أي استفسارات أو أية طلبات، ويمثل هذا التهديد خطرًا على الشركات التي تعتمد على المقر الإلكتروني في التجارة[1].

- **استخدام المقر المعلوماتي للشركة كقاعدة لتنفيذ أعمال إجرامية:**

تتعرض مقار الشركات المتوسطة والصغيرة لهذا النوع من

الأمريكية في بكين، ونشر صورة للرئيس الأمريكي بشارب هتلري، ولقد أصاب القاتل الإلكتروني الصيني هدفه وسبب إزعاجًا كبيرًا، إلا إنه لاقى على الرغم من استمرار اختفائه عن الأنظار استحسان السياسيين الصينيين، وفي 17 / 7 / 2000 وفي تمام الساعة 48: 13 أعلنت مؤسسة I C N قيام شرطة لونج أيلاند بالقبض على أحد المشتبه في عضويتهم لمجموعة عصابية تقنية تدعى (SSH) Sesame street haxorz للاختراق عبر شبكة الإنترنت الذين اخترقوا شركة AMHERST Co. في نوفمبر 1999، والمشتبه به يبلغ من العمر خمسة عشر عامًا ومتهم باختراق أنظمة NASA مع مجموعة SSH وهو تلميذ بمدرسة ثانوية هي Rocky Point High School.

كذلك تناقلت وكالات الأنباء في يوم الاثنين 5 / 1 / 2001 قيام الهكرة من مُعادي العولمة الاقتصادية باختراق معلوماتي واختلاس معلومات سرية عن المنتدى وعن الرئيس الأمريكي الأسبق بيل كلينتون وعدد من قادة منتدى دافوس الاقتصادي، ثم أرسلوا هذه المعلومات في شكل أسطوانات مضغوطة تضم أيضًا أرقام كروت الائتمان الخاصة بهؤلاء القادة وأرقام الهواتف الناقلة الخاصة بهم... إلخ.

(1) د. أيمن عبد الحفيظ، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، مرجع سابق، ص 106.

الهجمات التي يمارسها هاكرز Hackers هواة أو مجرمون محترفون، حيث يستخدم المقر كنقطة انطلاق أعمال هجومية على مقار أخرى بحيث لا تستطيع المقار الأخرى اكتشاف هوية المهاجم الحقيقية أو موقعه الأساسي.

وفي هذا الصدد فإن مقر معلومات الشركة على شبكة الإنترنت يصبح بدون حماية أو حراسة، كما أن المجرمين يمكن أن يستخدموه لتنفيذ أعمال إجرامية، كالولوج لمواقع أخرى أو كقاعدة انطلاق لتنفيذ جرائمهم، أو لتغيير محتوى موقع آخر، أو لإخفاء مسروقاتهم.

كما يمكن استخدام مقر معلومات الشركات الذي لا يتضمن مستويات حماية مناسبة لإخفاء بعض الملفات وخصوصًا في حالات التجسس، وأخطرها التجسس الاقتصادي من خلال عناصر داخلية، فيستطيع الشخص أن يخفي ملفًا ما غير مسموح بتداوله على المقر لحين خروجه، ثم يقوم بالدخول إلى المقر من الخارج والحصول على الملف.[1]

- **تخريب المقر المعلوماتي للشركة:**

يتم ذلك من خلال عدة أعمال منها تغيير المحتوى، أو وقف الخدمة من خلال التحميل الزائد بإرسال الرسائل، كما يمكن أن يتم التخريب من خلال الدخول على البرامج الخاصة بإدارة المقر وتغيير بعض مكونات التشغيل بها، مما يؤدي إلى التوقف الكامل للمقر أو حدوث أخطاء في التشغيل.

وتعد المقار الحكومية الأكثر عرضة لهذا النوع من الهجوم، نظرًا لما تمثله تلك المقار والمعلومات الخاصة بها من أهمية إستراتيجية تعكس

(1) د. هلالي عبد اللاه أحمد، جرائم المعلومات عبر الحدود وأساليب مواجهتها وفق اتفاقية بودابست، دار النهضة العربية، القاهرة، 2008، ص 96.

صورة الإدارة[1]، ومازال هذا الأمر يمثل تحديًا للقوانين القائمة، والتي يصعب من خلالها مقاضاة مرتكبي مثل هذه الجرائم أو إصدار الأحكام عليهم.[2]

- **الدخول على النظم الداخلية للشركة:**

يمثل هذا الاعتداء مستوى من المخاطر أعلى درجة في تهديد الشركات التي يحدث فيها ارتباط بين مقر المعلومات الخاص بها ونظمها الداخلية، وهو بالتالي أكثر الأنواع تأثيرًا على التجارة الإلكترونية.

ويتم بدخول الهواة على أنظمة الشركة الداخلية من خلال أي جهاز يرتبط بشبكة الإنترنت ويرتبط في الوقت نفسه بالنظم الداخلية، وهو ما يشبه فتح الباب على مصراعيه لدخول أي عنصر إلى النظم الداخلية، وهو يمثل تهديدًا حقيقيًا للشركة حيث يتمكن الشخص الذي استطاع الدخول من الحصول على معلومات داخلية عن الشركة، مما يؤدي إلى نتائج سلبية في أعمال الشركة، بل قد يؤدي في بعض الأحيان إلى توقف الشركة كلية عن العمل، ومحو كل أو بعض المعلومات الداخلية للشركة، ويؤدي كذلك إلى فقد بعض المعلومات ذات الأهمية والتي قد تدخل في عمليات التجارة

(1) وقد تعرض مقر معلومات هيئة المخابرات الأمريكية CIA لهذا النوع من الهجوم، وتم تغيير الاسم إلى هيئة الغباء الأمريكية Central Stupidity Agency وذلك في سبتمبر 96، وقبلها بشهر كان مقر معلومات وزارة العدل الأمريكية قد تعرض لهجمة غيرت اسم المقر ليكون وزارة عدم العدل، وتم تغيير محتوى الصفحة الأساسية ليتضمن حالات وقضايا وأحكامًا تؤثر على صورة العدالة الأمريكية.

(2) د. عمر محمد أبو بكر بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مرجع سابق،ص 66, 67.

الإلكترونية، والتي من الصعوبة استعادتها[1].

ثانيا: مستويات تأمين مقار المعلومات:

يمثل الاعتداء على مقار التاجر الإلكتروني بفعل هجمات الهواة والمحترفين، والذين يمتازون بمهارات خاصة[2]، ومحاولتهم اختراق

(1) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، ص 355 وما بعدها.

(2) القضاء الأمريكي اعتمد معيار الهكترة بكونه تعبيراً عن المهارة الخاصة Special Skill، فالهكترة إذن هي مستوى مهاري خاص يتمتع به الهكرة، وهو مستوى يفيد في دلالته التعبير عن الكفاءة والصلاحية والأهلية التقنية التي يتمتع بها الهاكر، حيث يملك الجبروت في الاختراق وارتكاب أفعال تقنية عبر العالم الافتراضي لا يستطيع مباشرتها العامة من الناس حتى ولو كانوا يملكون خصيصة التعامل الحاسوبي.
ولقد أورد القاضي الأمريكي Kleinfeld تعريفا للمستوى المهاري الخاص هو "المستوى المهاري الذي لا يمكن التوصل إليه من قبل جمهور العامة، وعادة يتطلب تعليمًا إضافيا مع التدريب أو الحصول على ترخيص، ويمكن التمثيل لذلك بالطيارين والمحامين والأطباء والمحاسبين والصيادلة، وكذلك خبراء الجريمة".
ولقد كان أول بروز للمعيار القضائي / المهارة الخاصة في قضية الولايات المتحدة الأمريكية ضد بيترسين أمام القضاء الفيدرالي حيث أدين Justin Tanner Petersen وفقا للقسم 18 USC Sec. 1030 (a) (2) لقيامه بالهكترة لكونه - نتيجة لتمتعه بمهارات خاصة في التعامل مع الحوسبة والرقمية - مارس نشاطا تقنيا عالي المستوى تمثل في قيامه بممارسة النصب المعلوماتي باختراقه لنظم حاسوب مؤسسة كروت الائتمان National Credit Card Reporting Agency واختلاس بيانات شخصية عن المتعاملين بها واستغلال هذه البيانات في الحصول على كروت ائتمان، كما أنه اخترق حاسوب شركة الهاتف وتحكم في خطوط الهاتف المتصلة بالراديو Radio station وقام بتنظيم حصوله على جائزة تتكون من عدد اثنين سيارة Porsche قيمة كل واحدة 40,000 $ ورحلتين إلى جزر هاواي، ثم اخترق حاسوب مؤسسة الاقتراض التجارية الوطنية =

النظم الأمنية لمقار ونظم المعلومات والتي أصبحت اليوم واحدة من أكبر المشكلات التي تواجه مديري المعلومات في كافة المؤسسات والشركات، وبلغت تكاليف مواجهة هـذه المشكلة في الولايات المتحدة أكثر من 10 بلايين دولار وذلك في عام 1997، وتتزايد بمعدلات تصل إلى أكثر من 25% سنويا.

وتتنوع مصادر التهديد بين عناصر داخلية وخارجية بصورة جعلت مشكلة التأمين واحدة من أكبر المشكلات، حيث إن المخطط يجب أن يضع في اعتباره تقريبًا كل العوامل التي تهدد المقار، والمشاركين في هذا التهديد، والمستفيدين من المقر المهدد، والنظم السابقة في الحماية، وهو ما يضع أعباءً إضافية على المؤسسات والشركات في تصديها لهذه المشكلة.

= The National Commercial Lender's Computer وحصل لنفسه على 150,000 $ مودعًا إياها في بنوك عدة، ولقد جاء في حيثيات حكم الدائرة التاسعة "أن بيترسين يملك معرفة ومهارة غير عادية في كيفية عمل الحواسيب، وكيفية تخزين البيانات والحركة الاستردادية للمعلومة، وكيفية التحكم في النظام الأمني للحواسيب أو تجنب التعامل معه".
ولقد كانت من أهم القضايا التي ناقشت معيار المهارة الخاصة الذي يميز الهكرة عن غيرهم هي قضية الولايات المتحدة الأمريكية ضد Lee حيث ذهب القاضي Andrew J. Kleinfeld إلى ضرورة الاستناد إلى الكفاءة في تمييز المهارة الخاصة والهكترة وبالتالي الهكرة، وذلك وفقا للمعرفة غير العادية Extraordinary knowledge، فالهاكر يتمتع بمستوى مهاري خاص يمكنه من القيام بممارسة أنشطة خطرة حقا، مثل الاختراق والتعامل الحاسبي والرقمي بطريقة لا يمكن للعامة القيام بها، فلكي يمكن مباشرة الهكترة فإن ذلك يحتاج من الهاكر أن يلم بهذا المستوى المهاري الخاص.

– د. عمر محمد بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، مرجع سابق، ص 23.

ولقد تغيرت مفاهيم وضع خطط التأمين من النموذج التقليدي العادي والذي كان يعتمد على تحديد التهديدات، وقياس درجة تأثير كل تهديد، ثم تحديد إجراءات ومتطلبات مواجهة كل تهديد وتكلفة المواجهة، ثم تجميع كل هذه العناصر في خطة واحدة، تغير هذا المفهوم إلى مفهوم جديد يعتمد على بناء أنساق من مستويات التأمين تتكامل مع بعضها البعض في إطار واحد يحقق درجة تأمين مناسبة ضد غالبية أنواع التهديدات.

ويعد تأمين وحماية مواقع المعلومات على شبكة الإنترنت على عدة مستويات عملية طويلة الأمد، وليس مجرد شراء برنامج للحماية، ويتضمن مستويات الحماية الآتية:

1) **مستوى حوائط النيران Fire Walls**: وهو إحدى الوسائل لحماية الكمبيوتر من المتطفلين أو المقتحمين، حيث يعمل على منع الدخول غير المصرح به للجهاز، ويمكن أن يكون حائط النيران جهازًا Hardware أو برنامجًا، وربما يكون خليطًا من الاثنين، وفي شبكات المؤسسات الكبيرة تقوم حوائط النيران بالتحكم في سريان المعلومات في الاتجاهين الداخل والخارج، حيث تقوم بحماية مستخدمي الشبكة من الداخل من أي اقتحام خارجي، ولكنها في الوقت نفسه تقوم بمنع المستخدمين الداخليين من الوصول لأماكن ومعلومات غير مصرح لهم بها، وغالبًا ما تكون هذه المعلومات على شبكة الإنترنت[1].

2) **مستوى شبكة الاتصالات**: وتشمل حماية شبكات الاتصال التي تربط أجهزة التقنية بعضها ببعض محليًا ودوليًا، ولا تتيح فرصة اختراق النظم عبرها كما أنها بذاتها تكون محلا للاعتداء وموطنًا من مواطن

(1) at: www.megaclub.gov.eg/Content/Default.aspx

الخطر الحقيقي.

وإلى جانب هذين المستويين المهمين هناك العديد من المستويات الأخرى، كمستوى الحماية الخاصة بتشغيل الحاسب الموجود عليه مقر المعلومات، ومستوى المعلومات وقواعد البيانات الموجودة بالمقر، ومستوى أدوات وبرامج مواجهة الفيروسات، ومستوى الخطة العامة والسياسات الخاصة بتأمين وسلامة المعلومات، ومستوى الأفراد وتدريبهم.[1]

الفرع الثاني

حماية المستهلك الإلكتروني جنائيًّا

تبلور مفهوم الحماية الإلكترونية للمستهلك بعد اتساع مستخدمي شبكة الإنترنت في العالم، ويقصد به الحفاظ على حقوق المستهلك، وحمايته من الغش أو الاحتيال أو شراء بضائع مغشوشة باستخدام أدوات تقنية المعلومات، والتي تصل إلى كل مكان وتمارس تأثيرًا يتجاوز أحيانًا الأدوات التقليدية[2].

---

(1) يونس عرب، أمن المعلومات ماهيتها وعناصرها وإستراتيجياتها، بحث منشور على شبكة الإنترنت www.arablaw.org

(2) أغلب قوانين حماية المستهلك تنص على حقوقه وهي:

1. حق الأمان: حماية المستهلك من المنتجات وعمليات الإنتاج والخدمات التي تؤدي إلى مخاطر على صحته وحياته.

2. حق المعرفة: تزويد المستهلك بالحقائق التي تساعده على قيامه بالاختيار السليم، وحمايته من الإعلانات وبطاقات السلع التي تشمل معلومات مضللة وغير صحيحة.

3. حق الاختيار: أن يستطيع المستهلك الاختيار بين العديد من المنتجات والخدمات التي تعرض بأسعار تنافسية مع ضمان الجودة.

4. حق الاستماع إلى آرائه: أن تمثل مصالح المستهلك في إعداد سياسات =

وتكمن أهمية توفير الحماية للمستهلك في أنه الطرف الضعيف في التعاقد بينما المهنيون في مركز القوة، وأيضًا لأنه في التجارة الإلكترونية يكون التعاقد عن بعد، ولا يكون المنتَج محل التعاقد بين يدي المستهلك، وليست حماية المستهلك كغاية تبرر كل وسيلة قانونية تصبو إلى تحقيق هذه الغاية، فليس الأمر صراعًا بين طرفين بقدر ما هو ضبط للتوازن العقدي بينهما.

ونظرًا للمخاطر الكبيرة التي تنطوي عليها العملية الاستهلاكية في جميع مراحلها، وبصفة خاصة في مرحلة إبرام العقد الإلكتروني، ولوقاية المستهلك من مخاطر ما يقتنيه من سلع وخدمات، ولحمايته من شر الوقوع ضحية لنزعته الاستهلاكية، لذلك وجب على القانون أن يتعرض لحمايته في المعاملات الإلكترونية للوصول إلى الآليات اللازمة لإعادة التوازن في العلاقات الاستهلاكية بما يرفع الضرر والخطر عن المستهلك.

وليس ذلك على المستوى الوطني فقط، بل إن المعاملات الإلكترونية -

= الحكومة وتنفيذها، وفي تطوير المنتجات والخدمات.

5. حق إشباع احتياجاته الأساسية: أن يكون للمستهلك حق الحصول على السلع الضرورية الأساسية وكذلك الخدمات، كالغذاء والكساء والمأوى والرعاية الصحية والتعليم.
6. حق التعويض: أن يكون للمستهلك الحق في تسوية عادلة للمطالبة المشروعة، شاملة التعويض عن التضليل أو السلع الرديئة أو الخدمات غير المرضية.
7. حق التثقيف: أن يكون للمستهلك الحق في اكتساب المعارف والمهارات المطلوبة لممارسة الاختيارات الواعية بين السلع والخدمات، وأن يكون مدركًا لحقوق المستهلك الأساسية ومسئولياته وكيفية استخدامها.
8. حق الحياة في بيئة صحية: أن يكون للمستهلك الحق في أن يعيش ويعمل في بيئة خالية من المخاطر للأجيال الحالية والمستقبلية.

ولأنها في الغالب تكون معاملات دولية تتم عن طريق شبكة المعلومات الدولية شبكة الإنترنت - لا تعرف الحدود، ومن ثم فهي تمتد لتشمل كافة أرجاء المعمورة، مما يستدعي توحيد النظام القانوني الدولي[1]، بهدف التنسيق بين المراكز القانونية للمتعاقدين، واتساع نطاق الحماية القانونية للمستهلك.

واتسعت الحماية الإلكترونية للمستهلك لتشمل الخدمات البنكية والمصرفية[2]، فنظرًا لعدم تواجد أطراف العقد ومحله في مكان واحد، وضرورة سداد قيمة البضاعة أو الخدمة بصورة إلكترونية فقد يتعرض المورد أو المستهلك لمخاطر تتعلق بالاعتداء على سرية الأرقام الخاصة ببطاقات الائتمان، أو تحويل الأموال لغير الغرض المخصصة له، أو تحقق جريمة من جرائم الاعتداء على الأموال في صورتها التقليدية قبل إتمام التعاقد أو أثناء إبرام العقد أو بعد إبرامه، لذا فإن بعض المواقع تقوم بحل المشكلات الخاصة بالدفع والتسديد لتقليل خطر الاحتيال ببطاقات الائتمان أثناء الشراء من شبكة الإنترنت أو سرقة البيانات الشخصية.

ونتيجة لرغبة المجتمع الدولي وبصفة خاصة الأوروبي في حماية المستهلك وتشجيع التجارة الإلكترونية فقد توالت التوجيهات الأوروبية التي تؤكد أهمية توفير الحماية للمستهلك، كما تم الاعتراف في الكثير من الدول بالتوقيع الإلكتروني والقيمة القانونية للمعاملات الإلكترونية، وقد وردت

(1) في هذا الصدد، صدرت توجيهات المجلس الأوروبي Directive Council European بغرض توحيد قواعد حماية المستهلك بين الدول الأوروبية في مجال العقود المبرمة عن بعد.

(2) جميل حلمي، مقال بعنوان الحماية الإلكترونية للمستهلك، منشور على شبكة الإنترنت: www.al3ez.net/vb/showthread

مواد تتناول هذه الأمور في مشروع قانون التجارة الإلكترونية المصري، وفيما يلي نقدم تعريف المستهلك، ونبين المقصود بحمايته وبالأخص من الإعلانات المضللة، كما نبين الحماية المكفولة له وفقًا للمواثيق الدولية والتشريعات العربية.

أولا: تعريف المستهلك [1]:

يعرف المستهلك بأنه مركز جميع الأنشطة القانونية والاقتصادية التي أوجدها لنفسه وبنفسه كشريك في النظام الاقتصادي بعد أن عرف حقوقه ووزنه في السلسلة الاقتصادية بين شركائه فيها من منتجين وموزعين[2].

وعرف المجلس الأوروبي[3] المستهلك بأنه: " كل شخص طبيعي أو معنوي تباع له أشياء أو تؤدي له خدمات لاستخدامه الخاص ".

كما عرفه المجلس الاقتصادي الكندي بأنه: " هو الذي يستخدم السلع والخدمات النهائية التي يوفرها له المنتج والموزع ".[4]

(1) قام بتعريف المستهلك مؤتمر حماية المستهلك المنعقد في القاهرة في الفترة بين 7 إلى 9 مارس 1982 والذي نظمه اتحاد جمعيات التنمية الإدارية بالاشتراك مع الجهاز المركزي للتنظيم والإدارة، والمؤتمر المنعقد في مدنية فريبورج بألمانيا في الفترة من 20 إلى 23 سبتمبر سنة 1982, وهذان المؤتمران يميلان إلى الأخذ بالتعريف الذي تبناه المؤتمر الحادي والثمانون للموثقين المنعقد في مدينة ليون بفرنسا في الفترة من 12 إلى 15 مايو 1985، والذي لا يخرج عن عناصر هذا التعريف، مشار إليه في د. ميرفت عبد المنعم صادق، الحماية الجنائية للمستهلك، مرجع سابق، ص 3 وما بعدها.

(2) Raymond Thomas, Introduction Generale, 81 Congres des Notaires de France, Le Consommateur, Tome I, Lyon, 12.15 Mai 1985, p.13

(3) قانون حماية المستهلك، الصادر من البرلمان الأوروبي في 17 مايو 1973.

(4) Gilles Oury, Les acteurs de la consommation, 81 Congres des Notaires de France, ibid., p.36.

وعرف الفقهُ المستهلكَ بأنه: " الشخص الذي يحوز أو يستخدم سلعًا أو خدمات لغرض غير مهني ".[1]

والمستهلك في مجال معاملات التجارة الإلكترونية هو نفس المستهلك في مجال عمليات التعاقد التقليدية، ولكنه فقط يتعامل عبر وسيلة إلكترونية ومن خلال شبكة اتصالات عالمية، وهذا يعني أن للمستهلك الإلكتروني نفس حقوق المستهلك العادي، وأنه يتمتع بنفس الحماية القانونية التي يقررها له المشرع، مع الأخذ في الاعتبار القواعد الخاصة المتعلقة بخصوصية العقد الإلكتروني، وكونه من العقود التي تبرم عن بُعد عبر شبكة إلكترونية.

وقد اتجه جانب من الفقه إلى التوسع في مفهوم المستهلك، وذلك بغرض إدخال المهني أو المحترف ضمن فئة المستهلكين، فعرف المستهلك بأنه "كل من يبرم تصرفًا قانونيًا من أجل استخدام المنتج أو الخدمة في أغراضه الشخصية أو في أغراضه المهنية"، أما غالبية الفقه فيتجه لتبني مفهوم ضيق للمستهلك يكون فيه المستهلك كل من يقوم بالتصرفات القانونية اللازمة لإشباع حاجاته الشخصية والعائلية.

وقد عرف توجيه المجلس الأوروبي رقم (93/13) الصادر في 1993/4/5 بشأن الشروط التعسفية في العقود المبرمة مع المستهلك في المادة الثانية عقود الاستهلاك بأنها: "تلك العقود التي تبرم بين التاجر والمستهلك، والتي يبرمها هذا الأخير بصفة عامة لأغراضه الشخصية

---

(1) **Jean Calais،Auloy, Droit de la Consommation, 3e edition 1992, p.3**
،Herman Bekeart, Introduction' a L' etude de droit Bruxelles, Document du travail, Travaux de L' association Henri Capitant T.XXIV , édition 19, 1973, p.166

وليس لأغراض تجارية أو مهنية".[1]

كما قصر التوجيه الأوروبي الصادر عام 2000 مفهوم المستهلك على الشخص الطبيعي فقط دون الشخص الاعتباري.

ثانيًا: المقصود بالحماية وأنواعها:

تعني حماية المستهلك حفظ حقوقه وضمان حصوله على تلك الحقوق قِبَل المهنيين بكل صورهم، سواء أكانوا تجارًا أو صناعًا أو مقدمي خدمات أو شركات[2]، وهذه الحماية المطلوبة للمستهلك حماية قانونية تأخذ مظاهر وأساليب متعددة جنائية، أو تنظيمية، أو إدارية، أو مدنية، والواقع أن الحماية الجنائية للمستهلك هي أهم جوانب الحماية التي يكفلها المشرع لجمهور المستهلكين، وسوف نعرض لحماية المستهلك الإلكتروني في المواثيق الأوروبية، ومشروع قانون التجارة الإلكترونية المصري، وقانون حماية المستهلك بدولة الإمارات العربية المتحدة.

ثالثا: حماية المستهلك من الإعلانات المضللة:

إن الأعمال التجارية الإلكترونية تكون بصفة عامة مسبقة بشكل من أشكال الدعاية والإعلان عبر شبكة الإنترنت، ولاشك أن الإعلان أصبح من أهم آليات النشاط التجاري في المنافسة وتحقيق الربح عبر الشبكات الإلكترونية.

---

(1) **Consumer contracts are those concluded between a merchant and a consumer, this latter generally being a private person who contracts for purposes outside of his or her trade or profession. (Council Directive, 13/93, 5 April 1993).**

(2) **د. محمد عفيفي حمودة, مفهوم حماية المستهلك, بحث مقدم في ندوة حماية المستهلك نظمتها لجنة العلوم الإدارية بالمجلس الأعلى للثقافة بالقاهرة في 23 يونيه عام 1981, ص3.**

وقد يلجأ المهني أحيانًا إلى استخدام أساليب دعائية منطوية على غش وخداع وتضليل، بل وذكر مواصفات خاطئة وغير صحيحة للمنتج أو الخدمة المعلن عنها بقصد دفع المستهلك للتعاقد، فإذا كانت الرسالة الإعلانية كاذبة أو مضللة فإنها بلا شك ستؤثر على سلوك المستهلك وحريته في الاختيار، ولذلك كان من الأهمية بمكان بيان قواعد حماية المستهلك في مواجهة الإعلانات الإلكترونية.

وقواعد حماية المستهلك في هذا المجال تقوم على ثلاث قواعد رئيسية هي كالآتي: أولا: وضوح الإعلانات، ثانيًا: تجريم الإعلانات المضللة، ثالثًا: الرقابة على الإعلانات.

أ - اشتراط وضوح الإعلان الإلكتروني:

تبين غرفة التجارة الدولية بالمادة (11) من القانون الدولي بشأن التطبيقات السليمة للإعلان الالتزامات الواجب توافرها في الإعلان كالآتي "أن الإعلان يجب أن يكون مميزًا بصورة واضحة مهما كان الشكل أو الوسط المستخدم، وعندما يتم إذاعة الإعلان أو نشره في وسائل الإعلام media يجب أن يقدم بصورة يظهر منها فورًا أنه إعلان.[1]

وهناك مشكلة ترتبط بالقوانين المتعلقة بالإعلانات التي تصدر في الخارج وهي صعوبة الرقابة عليها من جهة، وتحديد القانون الذي تخضع له من جهة أخرى،فقد يكون الإعلان مسموحًا به في بلد معين بينما يكون ممنوعًا في بلد آخر، بل إن الإعلان قد يكون داخل البلد الواحد مسموحًا به في ولاية دون ولاية، كما هو الحال في الولايات المتحدة الأمريكية حيث نجد أن ألعاب القمار والمراهنات مصرح بها في ولاية لاس فيجاس مثلا،

---

(1) Art (11) of International Code of Fair Practice in Advertising from the international chamber of commerce.

بينما غير مصرح بألعاب القمار في ولاية نيويورك، وبالتالي يمتنع الإعلان عن أماكن لعب القمار في مدينة نيويورك.

ب - حماية المستهلك من الإعلان الإلكتروني المضلل:

1- ماهية الإعلان الإلكتروني المضلل:

يتوجه المعلن بالإعلانات التجارية إلى المستهلك النهائي، فإذا كانت مضللة فإنها توقعه في لبس، ولذلك يجب حماية المستهلك من الإعلانات التجارية المضللة عن كل ما يعرضه التاجر في الفاترينة الإلكترونية، إذ إن المستهلك قد يقع فريسة سهلة للإعلانات الخادعة، ولا يكتشف ذلك إلا بعد أن يكون قد دفع ثمن المنتج أو الخدمة محل الإعلان بل وربما استلمها أيضًا.

وقد عرف توجيه المجلس الأوروبي الصادر في 10 سبتمبر 1984 بالمادة الثانية منه الإعلان المضلل أو الخادع Misleading advertising بأنه "أي إعلان، بأي طريقة كانت، يحتوي في طريقة تقديمه على أي تضليل، أو قد يؤدي إلى تضليل لهؤلاء الذين يوجه أو يصل إليهم الإعلان".[1] كما نصت المادة الثالثة من التوجيه السابق على أن الإعلان المضلل يقع عن طريق إغفال إحدى الخصائص الجوهرية للسلعة المعلن عنها.

2 - أركان جريمة الخداع الإعلاني:

إن مناط عدم مشروعية الإعلان المضلل هو خداع المستهلك وما يرتبه

(1) Any advertising which in any way whatsoever, and including its presentation misleads or is likely to mislead the people to whom it is addressed or whom it reaches or which for these reasons, is prejudicial or is likely to be prejudicial to a competitor. ART 2 of the pre‹mentioned directive of September 10, 1984.

ذلك من آثار سلبية، وجريمة الخداع الإعلاني لا تقوم إلا إذا توافر لها ركنان أساسيان: الأول الركن المادي وهو التضليل، ويقصد به كل ما من شأنه إيقاع المتلقي في اللبس أو الخداع، والثاني هو الركن المعنوي وهو قصد المعلن خداع المتلقي من أجل حمله على التعاقد، وتضليل المستهلك في الرسالة الإعلانية قد يكون بفعل إيجابي من المعلن، كما يمكن أن يكون بالترك Omission أي باتخاذ موقف سلبي يمتنع فيه عن ذكر بيان جوهري بالسلعة محل الدعاية.

ج - حماية المستهلك من الإعلان الإلكتروني المقارن:

إن التضليل في الإعلان التجاري لم يعد قاصرًا على خداع المستهلك فقط، بل امتد لينال من قيمة سلع وخدمات المنشآت التجارية المنافسة، وذلك عن طريق ما يسمى بالإعلان المقارن Comparative-advertising الذي أصبح يلعب دورًا كبيرًا في تشويه منتجات المنافسين، ذلك لأنه قد يستهدف التقليل من قيمة السلع والمنتجات أو خدمات المنشآت المنافسة أو إيقاع المستهلك في لبس، وبالتالي يصبح أداة للمنافسة غير الشريفة، والإعلان التجاري المقارن إما أن يكون إعلانًا محطًا للقيمة أو إعلانًا مفضيًا إلى لبس.

وقد عرف التوجيه الأوروبي الصادر في 6 أكتوبر 1997[1] الإعلان المقارن بأنه: "كل إعلان يؤدي صراحة أو ضمنًا إلى التعرف على سلعة أو خدمات منافس آخر"، ولن يختلف الإعلان المقارن الإلكتروني عن هذا الإعلان إلا في أنه يتم عبر وسائط إلكترونية ومن خلال شبكة الإنترنت.

ولذلك اختلفت مواقف التشريعات بين المنع والإجازة للإعلانات المقارنة، فقد ذهبت بعض التشريعات إلى إجازة الإعلان المقارن باعتباره

(1) Directive 97/55/CE du 6 octobre 1997.

مفيدًا للمستهلك، مثل القانون الأمريكي والقانون الكندي، والقانون الأيرلندي، والقانون الهولندي والسويسري، وقوانين الدول الإسكندنافية (السويد والنرويج والدنمارك وفنلندا).

وتحظر تشريعات بعض الدول الإعلان المقارن نهائيًا، على أساس أنه من الخطورة بمكان أن يدخل في إطار المنافسة التعرض - سواء صراحة أو ضمنًا - لمنتجات أو خدمات منشآت تجارية منافسة، ومن هذه القوانين القانون الفرنسي والقانون الإيطالي والقانون الأسباني والقانون البلجيكي والقانون النمساوي وقانون لكسمبرج.

والإعلان التجاري المقارن مصدره المعلن نفسه، ولذا فإنه يقدم للمستهلكين معلومات غير دقيقة، حيث يلجأ المعلن بهدف تسويق منتجاته إلى إبراز مزاياها مقارنة بالسلع والخدمات المنافسة، ومع ذلك فإنه يجوز للمعلن أن يشير في إعلانه إلى استطلاع الرأي الذي تجريه بعض الجهات بشأن معدل بيع أو استهلاك سلع ومنتجات معينة.

رابعًا: الالتزام بإعلام المستهلك في العقد الإلكتروني:

من أهم المشكلات التي تثير قلق المستهلك وقد تحد من إقباله على إبرام عقود التجارة الإلكترونية هي عدم معرفة شخصية البائع، وللتغلب على هذه المشكلة فإن البعض يرى أن المطلوب هو إيجاد آليات قانونية وإدارية وتكنولوجية لإعطاء شهادة تدل على شخصية التاجر أو المورد عن طريق طرف ثالث محايد وموثوق فيه بتقديم الضمانات الكافية وتسجيل مراحل التعاملات الإلكترونية بين الطرفين.

وأيًا ما كان الأمر، وسواء كان التاجر أو المنشأة التجارية سبق لها القيام بالكثير من المعاملات الإلكترونية أو بدأت حديثًا، فإن الالتزام بإعلام المستهلك الإلكتروني يقوم على عنصرين أساسين: الأول معرفة وتحديد

شخصية البائع، والثاني بيان الخصائص الأساسية للسلع والخدمات والشروط العامة للبيع.

أ - معرفة وتحديد شخصية التاجر الإلكتروني:

من أهم الأمور التي تثير قلق المستهلك الإلكتروني هو عدم معرفة شخصية البائع الذي يتعامل معه، وذلك لأن تحديد شخصية البائع يوفر عنصر الأمان للمستهلك في مجال التعاقد الإلكتروني عبر الشبكات.

والعرض المقدم عبر صفحات الويب والخاص بالمنتجات والخدمات يجب أن يتضمن اسم المنشأة، وأرقام التليفونات الخاصة بها، وعنوان الشركة، ومقر المؤسسة المسئولة عن العرض وسجلها التجاري، وأن تتضمن الفواتير الخاصة بها الطلبات والأسعار والوثائق الإعلانية، ويجب أن تكون جميع مراسلاتها موقعة باسمها.

و قد أكد على ذلك التوجيه الأوروبي الصادر في 20 مايو 1997 أنه يجب تحديد شخصية البائع من خلال التمييز بين ثلاث حالات تتعلق بمكان الموقع عبر شبكة الإنترنت وهي حالة وجود موقع الويب في موطن المستهلك، والحالة الثانية خاصة بمواقع الدول الأعضاء، والحالة الثالثة بشأن المواقع المنشأة في البلاد الأجنبية.

ب - الخصائص الضرورية للسلع والخدمات والشروط العامة للبيع:

على التاجر الإلكتروني الذي يعرض منتجاته عبر شبكة الإنترنت أن يحدد الخصائص العامة الضرورية للمنتج أو الخدمة، وعلى وجه الخصوص الخصائص الكيفية والكمية والمدة التي ستعرض فيها قطع الغيار في السوق، والسعر شاملا الضرائب ورسوم التسليم وميعاده، ويجب على البائع أيضًا بيان مدة صلاحية العرض، وأنه يحق للمستهلك الرجوع عن التعاقد خلال مدة محددة من تاريخ تسلم المنتج أو من تاريخ العقد الخاص بالخدمات.

خامسًا: حماية المستهلك في المواثيق الدولية:

التوجيه الأوروبي في شأن حماية المستهلك في العقود عن بعد رقم 7/97 الصادر عن البرلمان الأوروبي والمجلس في 20 مايو 1997 يعد هو الأساس الذي تستند إليه التشريعات الأوروبية لتوفير الحماية القانونية للمستهلك عند إبرام عقود التجارة الإلكترونية، وبصفة خاصة بطريق شبكة الإنترنت[1].

وأكد التوجيه الأوروبي رقم 31/2000 الصادر في 8 يونيو 2000 بشأن التجارة الإلكترونية على ضرورة عمل الدول الأعضاء على أن تراعى الاتصالات التجارية من قبل شركات المعلومات قابليتها للتعرف عليها، وسهولة التعرف على الشركات التي تقدم هذه الخدمات، وإيضاح الشروط والمواصفات الخاصة بالتخفيضات والهدايا والتصفيات والألعاب والمسابقات (مادة 6)، كما يجب على الدول التي لا تمنع الرسائل الدعائية أن تعمل على أن يكون من يقوم بهذه الأفعال قابلا للتعرف عليه إذا كان موجودًا على إقليمها، وأن يراعي هذا الشخص طلبات المرسل إليهم بعدم رغبتهم في تلقي مثل هذه الدعاية (مادة 7)، وأوصى التوجيه بضرورة اطلاع المستهلكين على بيانات تتعلق بخطوات إبرام العقد وكيفية تصحيح الأخطاء قبل إتمام العقد، وشروط تقديم الطلب (مادة 10 و11).

وتؤكد التوصيات والتوجيهات الأوروبية ضرورة حماية المستهلك، وأهم هذه الوثائق المقترحات الخاصة بحماية المستهلك في مجال التجارة الإلكترونية، والتوجيه الأوروبي رقم 93/99 الصادر في 13 ديسمبر 1999 في شأن إطار أوروبي عام للتوقيع الإلكتروني، ويوضح ذلك اهتمام

(1) **Pierre Bouzat, La protection penale du consommateur, Lectures á études supérieures' a la Faculte du Droit d Alexandria, 1998, pp. 8,11.**

الاتحاد الأوروبي المتزايد وتركيزه في الفترة الحالية بالتجارة الإلكترونية، وبصفة خاصة وضع إطار عام للدول الأوروبية لتوفير حماية قانونية للمستهلك في مجال التجارة الإلكترونية.

ومن ناحية أخرى فقد صدرت مجموعة من التشريعات المتلاحقة لتوفير الحماية الإلكترونية بصفة خاصة للمستهلك، وأهم هذه التشريعات قانون لوكسمبورج والقانون الأيرلندي والقانون الإيطالي[1]، وصدر كذلك حديثًا القانون الفرنسي.

وانطوى قانون التجارة الإلكترونية لدوقية لوكسمبورج على نصوص لحماية المستهلك، وأهمها الحق في الإحاطة المسبقة بالمعلومات الخاصة بالمورد، وبمواصفات السلع والخدمات، والعملة التي يتم بمقتضاها السداد، ومدة العرض والسعر، وشروط القرض إذا كان ممكنًا، ووجود الحق في العدول من عدمه، وكيفية رد الثمن المسدد من قبل المستهلك حال عدوله، وشروط الضمان، وخدمات ما بعد البيع، ويجب أن تتواجد هذه المعلومات خلال جميع مراحل التعاقد (مادة 53) بحيث يستطيع المستهلك أن يتخذ قراره بعد الاطلاع على مواصفات البضاعة مع الاحتفاظ بحقه في العدول، وقد حدد المشرع هذا الحق بسبعة أيام بصفة عامة بالنسبة للعقود الإلكترونية، وتبدأ المدة من تاريخ العقد الخاص بالخدمات، أما بالنسبة للبضائع فتبدأ المدة من تاريخ استلام البضائع (مادة 55)[2].

كما ألزم قانون التجارة الإلكترونية الجديد بإيطاليا الموردين بإحاطة المستهلكين بالمواصفات التفصيلية للبضاعة أو الخدمة وسعرها بما في ذلك الضرائب في الوقت المناسب قبل إبرام العقد، وبما يسمح للمستهلك

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 16.
(2) د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، مرجع سابق، ص 25.

بالعدول.

كما أن هناك اهتمامًا عالميًا بحماية المستهلك، وتعددت الاتفاقيات الدولية لحمايته وإن كانت لا تتعلق مباشرة بذلك، ومن هذه الاتفاقيات اتفاقية بروكسل لعام 1968 بشأن تنفيذ الأحكام الأجنبية، واتفاقية لاهاي سنة 1978 بشأن القانون الواجب التطبيق على عقود الوساطة والتمثيل التجاري، واتفاقية فيينا بشأن البيع الدولي للبضائع لعام 1980، واتفاقية روما لسنة 1980 بشأن القانون الواجب التطبيق على الالتزامات التعاقدية.

كما ظهرت العديد من المبادرات الدولية في هذا الشأن، وعلى وجه الخصوص المتعلقة بوضع معايير موحدة، ومن هذه المبادرات ما أوصت به منظمة التعاون الاقتصادي والتنمية (OECD) من عمل توجيهات وإرشادات تتعلق بالخطوط العريضة لحماية المستهلك الإلكتروني Cyber Consumer، وذلك من خلال الهيكل العام للتجارة الإلكترونية.[1] ومن التوجيهات المقررة على سبيل المثال لحماية المستهلك في عقود التجارة الإلكترونية والتي أوصت بها منظمة التعاون الاقتصادي والتنمية:

1) يجب أن يكون هناك مستوى معين من الحماية للمستهلك الذي يكون طرفًا في عمليات تجارة إلكترونية أو عمليات بيع عن بعد.

2) أن تكون المعاملات واضحة للمستهلك وبلغة مفهومة له، وأن يذكر هوية الشركة التي تقوم بالأنشطة التجارية الإلكترونية، وكذلك نوع السلع والخدمات التي تقدمها.

3) تقديم معلومات شاملة عن العرض المقدم من المورد بما فيه ذلك

(1) Organization for Economic Co، Operation and Development, Electronic Commerce، Opportunities and Challenges for Government, 1998, p53.

تحديد الثمن وطريقة الدفع والضمانات المقدمة وطريقة تسليم المنتج.

4) الحصول على موافقة صريحة وواضحة من المستهلك.

5) إعطاء المستهلك مهلة مناسبة للتفكير في إتمام التعاقد أو العدول عنه.

6) التعريف بالقانون الواجب التطبيق على التعاقد الإلكتروني والمحاكم المختصة.

7) إنشاء وسائل لتوثيق المعاملات الإلكترونية فيما بين التاجر والمستهلك.

8) تطوير التعاون الدولي بين الدول والمنظمات الدولية المعنية بحماية المستهلك.

سادسًا: حماية المستهلك في مشروع قانون التجارة الإلكترونية المصري[1]:

(1) نص مشروع القانون العربي الاسترشادي للتجارة الإلكترونية على حماية المستهلك بقوله: (في العقود الإلكترونية المبرمة بين المهنيين والمستهلك يلتزم المهني قبل إبرام العقد بإعلام المستهلك بطريقة واضحة ومفهومة بالمعلومات الآتية:

- هوية وعنوان البائع.
- وصف مفصل لمراحل إنجاز المعاملة.
- طبيعة وخواص وسعر المنتج أو الخدمة.
- نفقات تسليم المنتج، ومبلغ تأمينه، والضرائب المستحقّة، وأية مبالغ أخرى.
- الفترة التي يكون خلالها المنتج معروضًا بالأسعار المحدّدة.
- البيانات الخاصة بخدمة ما بعد البيع، والضمانات التجارية المتوفّرة.
- طرق وإجراءات الدفع.
- طرق وآجال ومكان التسليم وتنفيذ العقد، والآثار المترتّبة على عدم تنفيذ الالتزامات.
- كيفية إقرار الصفقة.
- طرق إرجاع المنتج أو إبداله واسترداد المبلغ المدفوع، وأجله المحدّد.
- نفقات استعمال تقنيات الاتصال حين يتمّ استعمالها على أساس مختلف عن =

فرض مشروع التجارة الإلكترونية المصري على المعلن بطريق

= التعريفة الجاري العمل بها.

- شروط فسخ العقد.
- شروط وإجراءات استعمال حقّ العدول عن العقد.
- الحدّ الأدنى لمدة العقد فيما يخصّ العقود المتعلّقة بتزويد المستهلك بخدمة أو منتج خلال مدة طويلة أو بصفة دورية.

كما نص مشروع القانون على أنه يحظر على المهني تسليم منتج أو خدمة مشروط بطلب دفع إذا لم يتمّ التعاقد بشأنه مع المستهلك، وفي حالة تسليمهما لا يحقّ له مطالبة المستهلك بالثمن أو مصروفات الشحن أو التسليم، وقرر أنه يتعيّن على المهني قبل إبرام العقد تمكين المستهلك من المراجعة النهائية لجميع خياراته، وتمكينه من إقرار التعاقد أو تغييره حسب إرادته، وكذا الاطلاع على شهادة التوثيق الإلكترونية المتعلّقة بالتوقيع الإلكتروني، وأجاز للمستهلك العدول عن الشراء بالوسيلة التي تمّ بها الشراء وذلك في أجل محدّد..... يحسب من تاريخ تسلّم البضاعة ومن تاريخ إبرام العقد بالنسبة للخدمات، ويتعيّن على المهني ردّ الثمن في أجل......... من تاريخ إرجاع المنتج أو العدول عن الخدمة، ويتحمّل المستهلك تكاليف إرجاع البضاعة، وقرر أنه لا يجوز للمستهلك العدول عن الشراء في إحدى الحالات الآتية:

أ. عند توفير الخدمة ويكون حيّز التنفيذ بطلب من المستهلك قبل انتهاء أجل العدول عن الشراء.

ب. إذا تمّ تزويد المستهلك بمنتجات حسب مواصفات شخصية، أو منتجات لا يمكن إعادة إرسالها، أو تكون قابلة للتلف أو الهلاك أو الفساد.

ج. إذا قام المستهلك بنزع الأختام عن التسجيلات السمعية أو البصرية أو البرمجيات والمواد الإعلامية، أو إذا تمّ تحميل أي من هذه المواد آليا.

د. شراء الصحف والمجلات.

ورتب مشروع القانون على البائع أن يتحمل في حالة البيع مع التجربة الأضرار التي قد يتعرّض لها المستهلك، وذلك حتى انتهاء مدة تجربته، باستثناء حالات سوء الاستعمال، ويعتبر لاغيًا كل شرط للإعفاء من المسئولية يكون مخالفًا لذلك.

التجارة الإلكترونية التزامات معينة، وأهمها بيان اسمه وعنوانه والسلعة أو الخدمة والقيمة، وقيمة الجمارك التي تحصل عليها، ومكان وتاريخ التسليم، وجهة اعتماد التوقيع الإلكترونية، أخذًا في الاعتبار أن جذب المتعاقدين عن طريق شبكة الإنترنت تصاحبه في كثير من الأحيان دعايات كاذبة ومبالغات لا يستطيع المتعاقد تقديرها إلا بعد التعاقد وعند استلام السلعة أو بدء تقديم الخدمة، لذلك فقد وضع هذا النص لإلزام المعلن بما أفصح عنه من معلومات أو قدمه من بيانات في الإعلان، ويتيح هذا النص إبطال العقود التي تقع على سلع أو خدمات تختلف مواصفاتها أو شروط التعاقد بشأنها عما ورد في الإعلانات المتعلقة بها(مادة 15)[1].

كما فرض تحديد مدة للاحتفاظ بالبيانات الشخصية وعدم التعامل فيها بمقابل وبدون مقابل إلا بموافقة صريحة كتابية من صاحب الشأن, كما أضفى تكييفا على العقود النمطية المبرمة إلكترونيا واعتبرها عقود إذعان وأجاز ابطال ما يرد فيها من شروط تعسفية (مادة 17)[2]، وأعطى المستهلك الحق في فسخ العقد خلال مدة معينة، وقد حرص المشرع على عدم تعارض نصوص هذا القانون مع التزامات مصر الدولية في ضوء ما صادقت عليه مصر من اتفاقيات دولية متعلقة بالمعاملة الضريبية والجمركية والتجارية، وكذلك حرصًا على عدم إهدار المزايا الضريبية

(1) نصت المادة (15) من مشروع قانون التجارة الإلكترونية المصري على أنه: " تعتبر الإعلانات ووثائق الدعاية المرسلة أو المبثوثة عن طريق وسائط إلكترونية وثائق تعاقدية مكملة للعقود التي يتم إبرامها للحصول على السلع والخدمات المعلن عنها، ويلتزم أطراف التعاقد بكل ما ورد فيها" .

(2) نصت المادة (17) من مشروع قانون التجارة الإلكترونية المصري على أنه: "تعتبر العقود النمطية المبرمة إلكترونيا من عقود الإذعان في مفهوم القانون المدني من حيث تفسيرها لمصلحة الطرف المذعن، وجواز إبطال ما يرد فيها من شروط تعسفية".

والجمركية التي قررها المشرع من أجل تشجيع الاستثمار في مصر[1] وقد وردت الفقرة الثانية مؤكدة عدم إخلال هذا لقانون بأي نص في قانون آخر يقرر امتيازات أو إعفاءات ضريبية أو جمركية (مادة 20)[2].

سابعًا: حماية المستهلك في القانون الإماراتي:

أ- حماية المستهلك في القانون الاتحادي رقم24 /2006 بشأن حماية المستهلك:

قانون حماية المستهلك في مادته الأولى من الباب الأول يعرف المستهلك بأنه كل من يحصل على سلعة أو خدمة بمقابل أو بدون مقابل إشباعا لحاجته الشخصية أو حاجات الآخرين، وعرف المزود بأنه كل شخص طبيعي أو معنوي يقدم الخدمة أو المعلومات أو يصنع السلعة أو يوزعها أو يتاجر بها أو يبيعها أو يوردها أو يصدرها أو يتدخل في إنتاجها أو تداولها، وعرف المعلن بأنه هو كل من يعلن عن السلعة أو الخدمة أو يروج لها باستخدام مختلف وسائل الإعلان والدعاية.

وفي الباب الخامس أورد حقوق المستهلك، ومنها الحصول على تعويض وتسوية عادلة لمطالبه المشروعة، كالتعويض عن التضليل أو السلع الرديئة

(1) د. فؤاد جمال عبد القادر، إطلالة على مشروع قانون التجارة الإلكترونية، منشور على شبكة الإنترنت بالموقع: http://www.tashreaat.com

(2) نصت المادة (20) من مشروع قانون التجارة الإلكترونية المصري على أنه: "لا تخل أحكام هذا القانون بالاتفاقيات الدولية المتعلقة بالمعاملة الضريبية والجمركية والتجارية وغيرها المبرمة بين مصر والدول الأجنبية والمنظمات الدولية أو الإقليمية، كما لا يخل هذا القانون بالإعفاءات والمزايا الضريبية والجمركية المقررة بمقتضى قوانين الضرائب والجمارك وحوافز الاستثمار وغيرها من القوانين."

أو الخدمات غير المرضية، ويتطلب ذلك خدمات ما بعد البيع وتوفير الضمان لمدة معينة؛ لأن ذلك سيعزز من ثقة المستهلك في تعامله مع السوق، ويوفر درجة من الاستقرار، إضافة إلى حقه في إعادة السلعة إن وجد بها عيبًا يخل بها.

وبناءً على المادة رقم (4) من القانون الاتحادي رقم (24) لسنة 2006 تتولى إدارة حماية المستهلك ممارسة اختصاصات الإشراف على تنفيذ السياسة العامة لحماية المستهلك بالتنسيق مع الجهات المعنية في الدولة، والتصدي للممارسات التجارية غير المشروعة والتي تضر بالمستهلك، والتنسيق والتعاون مع الجهات المعنية في نشر الوعي الاستهلاكي في الدولة حول السلع والخدمات، وتعريف المستهلكين بحقوقهم وطرق المطالبة بها، ومراقبة حركة الأسعار والعمل على الحد من ارتفاعها، والعمل على تحقيق مبدأ المنافسة الشريفة ومحاربة الاحتكار، وتلقي شكاوى المستهلكين واتخاذ الإجراءات بشأنها أو إحالتها للجهات المختصة، ويجوز أن تقدم الشكوى من المستهلك مباشرة، كما يجوز تقديمها من قبل جمعية حماية المستهلك باعتبارها ممثلة للمشتكي، وتتولى أيضًا نشر القرارات والتوصيات التي تساهم في زيادة وعي المستهلك.

وفي الباب السادس حدد القانون عقوبات على مخالفة أحكامه، فجاء نص المادة (18) يقضي بأنه: "مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر، يعاقب بالغرامة التي لا تقل عن ألف درهم كل من يخالف أحكام هذا القانون والقرارات الصادرة تنفيذًا له، وإذا لم ينبه المزود إلى خطورة استعمال السلعة أو الخدمة بشكل ظاهر ونتج عن ذلك ضرر كانت العقوبة الغرامة التي لا تقل عن عشرة آلاف درهم ".

وفي المادة 19 أعطى القانون للمحكمة([1]) في حالة الحكم بالإدانة في إحدى الجرائم المشمولة بأحكام هذا القانون أن تقضي - فضلا عن العقوبة المقررة - بمصادرة أو إتلاف المنتج موضوع الجريمة والمواد والأدوات المستخدمة في إنتاجه.

ب- حماية المستهلك في القانون الاتحادي رقم2006/1 بشأن المعاملات والتجارة الإلكترونية:

لم يرتب القانون أحكاما خاصة حماية المستهلك, ولم يرد المستهلك الإلكتروني ضمن التعريفات الواردة بهذا القانون، ولكنه عرف المرسل إليه والذي يعد في قانون التجارة الإلكترونية أنه الشخص الطبيعي أو المعنوي الذي قصد المنشئ توجيه رسالته إليه، ولا يعتبر مرسلا إليه الشخص الذي يقوم بتزويد الخدمات فيما يتعلق باستقبال أو معالجة أو حفظ المراسلات الإلكترونية.

ولم يختلف مفهوم المستهلك في مجال التجارة الإلكترونية عنه في مجال التجارة التقليدية إلا في التعامل عبر الوسائل الإلكترونية والتقنية وشبكة الإنترنت.

لذا فإن المستهلك الإلكتروني له نفس حقوق المستهلك العادي، ويتمتع بنفس الحماية القانونية التي قررها المشرع في القانون 2006/24، مع الأخذ في الاعتبار القواعد الخاصة في خصوصية إبرام العقد عبر الوسائل الإلكترونية , وكان يتعين على المشرع في هذا المجال أن ينص على أحكام خاصة للمستهلك الإلكتروني لاختلافه عن المستهلك التقليدي, وإيجاد

---

(1) أصدر وزير العدل قراراً بإنشاء دوائر متخصصة في المحاكم الاتحادية الابتدائية للنظر في القضايا الجزائية الخاصة بحماية المستهلك، يعمل به اعتبارا من 27 إبريل 2009.

نصوص جنائية تضفي حماية على المستهلك الإلكتروني من أية مخاطر قد تعتريه في عملية التجارة الإلكترونية.

ثامنًا: حماية المستهلك في القانون التونسي:

يعد القانون التونسي الخاص بالمبادلات والتجارة الإلكترونية، من القوانين العربية القليلة التي أضفت حماية على المستهلك الإلكتروني، حيث نص في المادة (25) منه على أنه: (يجب على البائع في المعاملات التجارية الإلكترونية أن يوفر للمستهلك بطريقة واضحة ومفهومة قبل إبرام العقد المعلومات التالية:

- هوية وعنوان وهاتف البائع أو مسدي الخدمة.
- وصفا كاملا لمراحل إنجاز المعاملة.
- طبيعة وخاصيات، وسعر المنتوج.
- كلفة تسليم المنتوج، ومبلغ تأمينه، والادعاءات المستوجبة.
- الفترة التي يكون خلالها المنتوج معروضًا بالأسعار المحددة.
- شروط الضمانات التجارية والخدمة بعد البيع.
- طرق وإجراءات الدفع، وعند الاقتضاء شروط القروض المقترحة.
- طرق وآجال التسليم وتنفيذ العقد ونتائج عدم إنجاز الالتزامات.
- إمكانية العدول عن الشراء وأجله.
- كيفية إقرار الطلبية.
- طرق إرجاع المنتوج أو الإبدال، أو إرجاع المبلغ.
- كلفة استعمال تقنيات الاتصالات حين يتم احتسابها على أساس مختلف عن التعريفات الجاري بها العمل.
- شروط فسخ العقد إذا كان لمدة غير محدودة أو تفوق السنة.
- المدة الدنيا للعقد في ما يخص العقود المتعلقة بتزويد المستهلك بمنتوج

أو خدمة خلال مدة طويلة أو بصفة دورية.

يتعين توفير هذه المعلومات إلكترونيًا، ووضعها في حوذة المستهلك للاطلاع عليها في جميع مراحل المعاملة).

كما منع القانون على البائع تسليم منتوج مشروط بطلب دفع، لم تصدر بشأنه طلبية من قبل المستهلك، وفي حالة تسليم منتوج إلى المستهلك لم تصدر بشأنه طلبية، لا يمكن مطالبة هذا الأخير بسعره أو كلفة تسليمه، كما ألزم البائع قبل إبرام العقد بتمكين المستهلك من المراجعة النهائية لجميع اختياراته، وتمكينه من إقرار الطلبية أو تغييرها حسب إرادته، وكذلك الاطلاع على شهادة المصادقة الإلكترونية المتعلقة بإمضائه، واشترط القانون على البائع أن يوفر للمستهلك عند الطلب خلال العشرة أيام الموالية لإبرام العقد وثيقة كتابية أو إلكترونية تتضمن كافة المعطيات المتعلقة بعملية البيع.

كما أجاز القانون التونسي للمستهلك العدول عن الشراء في أجل عشرة أيام عمل، تحتسب بالنسبة إلى البضائع بداية من تاريخ تسلمها من قبل المستهلك، وبالنسبة إلى الخدمات بداية من تاريخ إبرام العقد، ويتم الإعلان بالعدول بواسطة جميع الوسائل المنصوص عليها مسبقا في العقد، وفي هذه الحالة يتعين على البائع إرجاع المبلغ المدفوع إلى المستهلك في أجل عشرة أيام عمل من تاريخ إرجاع البضاعة أو العدول عن الخدمة، ويتحمل المستهلك المصاريف الناجمة عن إرجاع البضاعة.

المطلب الثالث

حماية وسائل الدفع الإلكتروني

يعتبر الائتمان إضافة مستقبلية للأموال المشمولة بالحماية، بحيث تضمن هذه الإضافة كل التصرفات المالية للشخص، والمبدأ الأساسي في الائتمان هو الحماية، إذ برز الائتمان على إثر تصاعد حدة جرائم السرقة بالإكراه، والتي وصلت إلى أعلى معدلاتها في العدوان على الحياة في مقابل نهب المال من الضحايا، فالهدف يظل هو اختلاس الأموال، إلا أن السارق فضلا عن كونه يستخدم الإكراه فإنه كذلك يفضل ألا يترك أثرًا وراءه يمكن أن يقود إليه.

وعلى الرغم من كون قاعدة الحماية هي الأموال فإن الجريمة استطالت أيضًا الائتمان لكون الأموال عبر الائتمان تتحول إلى أرقام موضوعة على كروت يستلمها المؤتمن من المصرف الذي يتعامل معه[1].

ويعد الائتمان المتعامل به في العالم المادي وسيطًا لكونه يحل محل النقود في التعامل، ولكنه لا يمكن اعتباره وسيطًا عبر شبكة الإنترنت، لأنه يعد أحد أشكال السداد كالنقود، ذلك أن ما يتم عرضه للسداد عبر شبكة الإنترنت ليس الكارت الذي يثبت وجود الائتمان، وإنما رقم التعامل الائتماني الموضوع على الكارت ويسدد به الثمن، وسوف نتناول هذا المطلب على فرعين: الأول للمخاطر المصرفية والاعتداء على بطاقات الدفع، والفرع الثاني لحماية وسائل الدفع الإلكتروني.

---

(1) د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان، دار النهضة العربية، القاهرة، 1999، ص 5.

الفرع الأول

المخاطر المصرفية والاعتداء على بطاقات الدفع

يتم سداد القيمة إلكترونيًا وتسوية المدفوعات المتعلقة بالصفقة، حيث يقوم المستهلك بملء نموذج الشراء بعد اختياره للمنتج الذي يحتاج إليه، ويشمل النموذج رقم البطاقة الائتمانية الخاصة به، وقيمة البضائع المشتراة، وتنقل هذه البيانات بواسطة الحاسب الآلي ومعها رقم بطاقة الائتمان إلى الحاسب الآلي الخاص بالبنك الذي يتعامل معه التاجر، ويقوم البنك بالتحقق من صحة هذه البيانات، ثم يقوم الحاسب الآلي بالبنك بخصم قيمة البضائع المشتراة من حساب المشتري، ثم إضافتها إلى حساب البائع حتى ولو في بنك آخر غير بنك المشتري، وتستخدم النقود الإلكترونية[1] عبر شبكة الإنترنت في سداد القيمة، حيث يقوم البنك بإصدار نقود إلكترونية لعملائه، ويحتفظ العميل بالنقود الإلكترونية في محفظة إلكترونية يتم حفظها على القرص الصلب، أو يتم التحفظ عليها في ذاكرة البطاقات الذكية، وتعتبر الشيكات الإلكترونية من أهم وسائل الدفع التي تعتمد على الحاسب الآلي، حيث ينتقل الشيك بالبريد الإلكتروني إلى المستفيد بعد توقيعه إلكترونيًا، فيحصل عليه المستفيد ويوقعه إلكترونيًا، ويرسله بالبريد الإلكتروني مصحوبًا بإشعار وإيداع إلكتروني في حسابه بالبنك.

ويجمع خبراء البرمجيات والمعلومات على أن وسائل الدفع الآمنة عبر شبكة الإنترنت لا تزال من أهم المشكلات والعقبات التي تواجه التجارة

(1) عرف مشروع القانون العربي الاسترشادي للمعاملات والتجارة الإلكترونية, النقود الإلكترونية بأنها وحدات نقد إلكتروني يمكن حفظها على مرتكز إلكتروني لمدة محددة، وتصدر مقابل نقد يتم مبادلته فورًا, بنفس القيمة ونفس العملة، وتتيح للغير دون المصدر إتمام عملية الدفع.

الإلكترونيـة في الـوطن العـربي، مؤكـدين ضرورة التعـاون بـين الحكومـات وشركـات تكنولوجيـا المعلومات لإيجاد الحلول المناسـبة والممتـازة للـدفع الآمـن عـبر شـبكة الإنترنـت، ورغـم الاتجـاه المتزايد نحو التجارة الإلكترونية في الـوطن العـربي إلا أنهـا لم تـرق بعـد إلى المسـتويات والمعـايير العالمية، وذلك بسبب تخوف المستثمرين من التعامل ببطاقاتهم الائتمانية لعدم اقتناعهم بوجود حماية كافية لهذه المواقع التجارية تحول دون اختراقها.

وتعد البطاقات الائتمانية[1] أكثر البطاقات الإلكترونية عرضة للسرقة والتزوير وغيرهـا مـن الجرائم التي تقع على الأموال، وأهم تلك الجرائم وأكثرهـا شـيوعًا السـطو عـلى أرقـام البطاقـات الإلكترونية من الشبكة العنكبوتية، واستخدامها في الحصول على السـلع، أو تحويـل المبـالغ التـي تحتويها هذه الحسابات إلى حسابات أخرى، وذلك بعد أن بدأ مفهوم التجارة الإلكترونيـة ينتشر لسهولة الاتصال بين الطرفين، ولإمكانية اختزال العمليات الورقية والبشرية، فضلا عـن السرعة في إرسال البيانات وتخفيض تكلفة التشغيل، والأهم هو إيجاد أسواق أكثر اتسـاعًا, وسـوف نتطـرق للمخاطر المصرفية، ومظاهر العدوان على بطاقات الدفع الإلكتروني، وطرق حمايتها، ما يلي:

أولا: المخاطر المصرفية:

ثانيًا: مظاهر العدوان على بطاقات الدفع الإلكتروني:

(1) تعود البداية الحقيقية لبطاقات الائتمان في مفهومها الحديث إلى العـام 1950 عـلى يـد الأمـريكيين فرانـك بكن مارا ورالف سيندر.

Drury.Ac.Ferrier ,CW Ccredit Card , London,Butter Wrth 1984 p15.

أولا: المخاطر المصرفية:

يصاحب تقديم العمليات المصرفية الإلكترونية مخاطر متعددة، وقد أشارت لجنة بازل للرقابة المصرفية[1] إلى أنه ينبغي أن تقوم البنوك بوضع السياسات والإجراءات التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها، وأصدرت اللجنة خلال مارس 1998 ومايو 2001 مبادئ لإدارة هذه المخاطر شملت: مخاطر التشغيل، ومخاطر السمعة، والمخاطر القانونية، ومخاطر الائتمان، والسيولة، وسعر العائد، ومخاطر السوق.

مخاطر التشغيل:

وهي تشمل:

أ - عدم التأمين الكافي للنظم:

تنشأ هذه المخاطر عن إمكان اختراق غير المرخص لهم لنظم حسابات البنك بهدف التعرف على المعلومات الخاصة بالعملاء واستغلالها، سواء تم ذلك من خارج البنك أو من العاملين به، بما يستلزم توافر إجراءات كافية لكشف وإعاقة ذلك الاختراق.

(1) تم إنشاء لجنة بازل للرقابة على البنوك عام 1974 من قبل محافظي البنوك المركزية في مجموعة البلدان العشر، ويتمثل هدف المجموعة في وضع المعايير الرقابية السليمة حول العالم، وعليه قامت اللجنة بتطوير معايير وإرشادات رقابية بشأن كافة الموضوعات الرقابية في البنوك، وتختص المعايير والإرشادات التي صدرت عن اللجنة بمكافحة غسل الأموال، ومنع الاستخدام الإجرامي للنظام المصرفي، وكفالة المبادئ الأساسية للرقابة المصرفية الفعالة، والعناية الواجبة بشأن عملاء البنوك.

ب - عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة:

وهـي تنشـأ مـن إخفـاق الـنظم أو عـدم كفاءتهـا، مثـل بـطء الأداء لمواجهـة متطلبـات المستخدمين، وعدم السرعة في حل هذه المشكلات وصيانة الـنظم، وخاصـة إذا زاد الاعـتماد عـلى مصادر خارج البنوك لتقديم الدعم الفني بشأن البنية الأساسية اللازمة.

ج - إساءة الاستخدام من قبل العملاء:

ويحدث ذلك نتيجة عدم إحاطة العملاء بإجراءات التأميـن الوقائيـة، أو بسـماحهم لعنـاصر إجراميـة بالـدخول إلى حسـابات عمـلاء آخـرين، أو القيـام بعمليـات غسـل الأمـوال باسـتخدام معلوماتهم الشخصية، أو عدم اتباعهم إجراءات التأمين الواجبة.

2 - مخاطر السمعة:

تنشأ مخاطـر السمعة في حالة توافر رأي عام سـلبي تجـاه البنـك، الأمـر الـذى قـد يمتـد إلى التأثير عـلى بنوك أخرى، نتيجة عدم مقدرة البنك عـلى إدارة نظمـه بكفـاءة أو حـدوث إختراق مؤثر لها.

3- المخاطر القانونية:[1]

(1) حالات الاستخدام غير المشروع لبطاقة الدفع الإلكتروني معقدة ومركبة، ومتطورة تقنيًا، وهـي كثـيرة مـن حيث النوع يصعب حصرها في عدد معين، فهي ذات أشـكال وأسـاليب متنوعـة، مرتكبوهـا مختلفـون، وتصنيفها صعب، حيث إنها تعد من الجرائم المستحدثة، والتقنية متغيرة في أساليبها، تتطور في كـل يـوم، وتوضح التقارير الصـادرة عـن المركـز الـوطني لجـرائم (الياقـات البيضـاء) أن الاحتيـال ببطاقـات الـدفع الإلكتروني مشكلة تتفاقم، حيث بينت أنّ فيزا وماستر كـارد لحقـت بهـا خسـارة مقـدارها (110) مليـون دولار من عام 1980: 1995، وارتفعت هذه الخسارة بسـبب عمليـات الاحتيـال بعـد عـام 1995 حيـث وصلت إلى مليار وستمائة مليون =

= دولار سنويًا.

وهناك عدة طرق يتمّ من خلالها الحصول على بطاقات الدفع الإلكتروني واستخدامها بطريقة غير مشروعة وهي:

1- فقدان البطاقة (Lost Card): ويحدث عندما تضيع البطاقة، ومن ثم تستعمل بشكل احتيالي من قبل شخص آخر غير مخول، وفي عام 2001 شكل فقدان البطاقة (12.5%) تقريبًا من خسائر الماستر كارد العالمية.

2- سرقة البطاقة (Stolen Card): ويحدث عندما تُسرق البطاقة من خلال السطو على المنازل، أو سرقة المحافظ، وغيرها من الوسائل، واستعمالها لأغراض احتيالية، وقد شكلت سرقة البطاقة ما نسبته (23.5%) تقريبًا من خسائر الماستر كارد العالمية في عام 2001، والبطاقات المسروقة والمفقودة تشكل ما نسبته (46%) من مجمل خسائر الفيزا كارد عالميًا حسب تقرير الفيزا عام 1999.

3- تزوير البطاقة (Card Counter Feinting): ويتمّ ذلك بالتصنيع الكامل لبطاقة مزورة تحوي معلومات الحساب والتشفير والهولجرام، وأيضًا هناك عمليات إعادة تشفير بطاقات منتهية الصلاحية، أو مسروقة، أو مفقودة باستخدام معلومات حساب آخر، وقد بلغت خسارة الماستر كارد عالميًا في عام 2001 بسبب التزوير (28.6%) تقريبًا، و(32%) من خسائر الفيزا العالمية لعام 2002.

4- طلبات احتيالية (Fraudulent Applications): تقديم طلبات باطلة للحصول على بطاقة دفع إلكتروني باستخدام بطاقات هوية مزورة، أو عائدة لأشخاص آخرين، وقد شكل هذا النوع من الاحتيال ببطاقة الدفع الإلكتروني ما نسبته (5.1%) من خسائر الماستر كارد العالمية لعام 2001، ويستغرق هذا النوع من الاحتيال عشرين يومًا تقريبًا، ولا يعلم الشخص الذي سرقت هويته الشخصية، أو فقدت بوجود بطاقة وفاء باسمه حتى يطالبه البنك بالتسديد.

5- عدم استلام البطاقة (Never Received Issue)): هي عملية سرقة البطاقة قبل أن تصل إلى صاحبها، وتستعمل من قبل شخص آخر بشكل احتيالي، وتسرق البطاقة عادة من البريد، وقد وصلت خسائر الماستر كارد عالميًا عام 2001 نتيجة هذا النوع من الاحتيال (4.5%) تقريبًا من مجموع جرائم البطاقات.

6- الاحتيال دون وجود البطاقة (Card Not Present): تتم بـ "التسوق بالبريد، أو بالهاتف" (Mail Order/ Telephone Order) وهي الطريقة التي يستحوذ فيها=

تقع هذه المخاطر في حالة انتهاك القوانين أو القواعد أو الضوابط المقررة، خاصة تلك المتعلقة بمكافحة عمليات غسيل الأموال، أو نتيجة عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات

= المستخدمون على معلومات الحساب بطريقة غير شرعية، وبعد ذلك تستخدم هذه المعلومات لطلب شراء بضائع أو خدمات عن طريق الهاتف، أو البريد أو شبكة الإنترنت، أو أية حالات أخرى لا تتطلب وجود البطاقة نفسها، بل يكفي استخدام رقمها الظاهر ومعلوماتها، وقد شكل الاحتيال بدون وجود البطاقة ما نسبته (23%) من خسائر الماستر كارد العالمية من مجموع الاستخدامات غير المشروعة لبطاقة الدفع الإلكتروني لعام 2001.

7- الطبع المتعدد (Multiple Imprint): ويحدث ذلك عندما يقوم التاجر أو الموظف في المحل التجاري عند الشراء بطبع البطاقة عدة مرات باستخدام الجهاز القارئ للبطاقة، حيث إنه يجب طبع البطاقة مرة واحدة لكل عملية شراء، ليلتقط الجهاز المعلومات المشفرة، فعندما يطبع التاجر البطاقة عدة مرات فإنّه بذلك يستطيع أن يسجل بضائع إضافية على حساب هذه البطاقة، ويحصل هذا النوع من الاحتيال عادة عند استخدام الأجهزة اليدوية، ولقد أصبحت الخسائر الناجمة عن الاحتيال بالطبع المتعدد تقل يومًا بعد يوم نتيجة انتشار الأجهزة الإلكترونية في المحال التجارية، وقد وصلت نسبة خسائر الماستر كارد العالمية عام 2001 نتيجة الطبع المتعدد (0.2%) تقريبًا، وقد بقيت نسبة الخسائر مستقرة تقريبًا حتى الربع الأول من عام 2004.

8- الاستيلاء على الحساب:Account Takeover)) وهي العملية التي بموجبها يقوم المستخدم بالاتصال بمصدري البطاقة للإبلاغ عن تغيير العنوان لبطاقة سارية عائدة لأشخاص آخرين، حيث يكون لدى المستخدم معلومات عن الحساب، وبعد ذلك يقوم بالاتصال بمصدر البطاقة للإبلاغ عن فقدانها وطلب بطاقة بديلة، والنتيجة النهائية إصدار بطاقة جديدة مع رقم سري جديد يتمّ إرسالها على العنوان الجديد، وبذلك يتمّ الاستحواذ على الحساب، وقد شكل هذا النوع من الاستخدام غير المشروع لبطاقة الدفع الإلكتروني ما نسبته (23%) من خسائر الماستر كارد العالمية لعام 2001.

المصرفية الإلكترونية، ومن ذلك عدم وضوح مدى توافر قواعد لحماية المستهلكين في بعض الدول، أو لعدم المعرفة القانونية ببعض الاتفاقيات المبرمة بشأن استخدام وسائل الوساطة الإلكترونية.

4 - المخاطر الأخرى:

يرتبط أداء العمليات المصرفية الإلكترونية بالمخاطر الخاصة بالعمليات المصرفية التقليدية، ومن ذلك مخاطر الائتمان والسيولة وسعر العائد ومخاطر السوق، مع احتمال زيادة حدتها، فعلى سبيل المثال فإن استخدام قنوات غير تقليدية للاتصال بالعملاء وامتداد نشاط منح الائتمان إلى عملاء عبر الحدود قد يزيد من احتمالات إخفاق بعض العملاء في سداد التزاماتهم.

ثانيًا: مظاهر العدوان على بطاقات الدفع الإلكتروني:

إن لكل كارت ائتمان عنوانًا فرديًا خاصًا يتميز به عن غيره، تمنحه المؤسسة المالية للمشترك لديها في هذه الخدمة، بحيث تحل محل التعامل بالأموال السائلة[1].

---

(1) شرطة دبي ضبطت مؤخرًا عصابة نيجيرية استولت على رصيد امرأة أوكرانية، كانت تودع مبلغًا ماليًا في حسابها الشخصي في أحد بنوك الدولة يقدر بنحو 200 ألف درهم، وتوجهت إلى بلادها في منتصف العام الماضي، وحين عادت في بداية العام الجاري فوجئت بأن رصيدها قد نفد تمامًا, وتوصلت المباحث الإلكترونية إلى أن الرصيد تم اختراقه من خلال الإنترنت، ونقلت الأموال الموجودة فيه على دفعات إلى حساب مختلف في بنك آخر, وتم التوصل إلى هوية صاحب الحساب الذي نقلت إليه الأموال، لكن تبين أن أوراقه غير صحيحة وأن هناك شخصًا آخر يدير هذا الحساب، وبمواصلة التحريات استنادًا إلى المعلومات التي توافرت من البنك توصلت المباحث إلى الشخص الذي يدير الحساب, وأوضحت شرطة دبي أن اختراق الحساب البنكي من خلال الإنترنت لا يمكن أن يحدث من دون تسرب =

= معلومات خصوصًا البيانات السرية للضحية سواء كان اسم التعريف أو كلمة المرور، وقد تم فحص جهاز الكمبيوتر الخاص بالمرأة الأوكرانية التي تعرض حسابها للسرقة لكن لم يتم العثور على شيء، وأوضحت أنه ربما استخدمت جهاز كمبيوتر غير آمن في أحد مقاهي الإنترنت أو أثناء وجودها في بلادها, وقد تم ضبط عدد من البطاقات الائتمانية المزورة لدى أفراد العصابة، وأنهم كانوا بصدد تغذيتها بالبيانات.

وتشتري العصابات المتخصصة في هذا النوع من الجرائم معلوماتها من تلك السوق وتستخدمها في تغذية البطاقات المزيفة وتنفيذ معاملات من دول مختلفة خصوصًا أن استخدام البطاقة يتجاوز الحدود ولا يحتاج سوى ماكينة صراف إلي، وقد أغلقت الولايات المتحدة إحدى هذه الأسواق, وأسعار البيانات التي تباع في السوق السوداء تختلف حسب نوع البطاقة وفترة صلاحيتها، فإذا كانت منتهية الصلاحية يكون سعرها رخيصًا للغاية، لكن إذا كان مفعولها ساريًا فتباع بمبالغ كبيرة.

ومن وسائل الحماية التي يمكن أن تستخدمها البنوك لتجنب حدوث أي اختراق لأرصدة عملائها هو تطبيق نظام الرقم المتغير للبطاقات بعد إجراء أي معاملة، وهو نظام يسير وربما يكون مكلفًا بعض الشيء، لكن سيوفر على المصرف الكثير من المخاطر، وهو عبارة عن جهاز صغير أشبه ببطاقة التخزين الإلكترونية «فلاش ميموري» يغير الرقم السري للعميل بعد إجراء المعاملة مباشرة.

وهناك خطورة من استخدام البطاقات الائتمانية في معاملات تجارية عبر الإنترنت خصوصًا من أجهزة غير آمنة، بل إن الجهاز الشخصي ذاته ربما لا يكون آمنًا إذا لم يكن مزودًا ببرنامج حديث مضاد للفيروسات، كما يحذر من ارتياد مواقع بعينها يزرع القائمون عليها برامج تجسس مثل المواقع الإباحية أو المواقع التي تعرض تنزيل البرامج الحديثة أو الأفلام والأغاني مجانًا، ومن غير المنطقي أن تطرح جهة تلك البرامج أو المنتجات مجانًا إذا لم يكن لديها غرض آخر, وهناك شركات عالمية كبرى تزرع في بعض المواقع «ميل وير» وهو نوع من برامج التجسس التي تستخدمها لقياس سلوكيات المستهلك وميوله تجاه سلعة معينة.

وهناك عصابات تقوم كذلك بزرع أجهزة تجسس في مقاهي الإنترنت تقوم بسرقة بيانات الأشخاص الذين يرتادون تلك الأماكن ويستخدمونها بعد ذلك في إجراء معاملاتهم, ويشار إلى أن هذا النوع من الجرائم يعرف باسم «419»، وأطلق =

والشكل المادي لكروت الائتمان يتمثل في تلك البطاقات البلاستيكية الموصوفة بمقاييس معينة، وأما نطاق استخدامها فيختلف بحسب نوعية الخدمة التي تستخدم فيها، فكما أن هناك بطاقات تستخدم لسحب مبالغ مالية من آلات توفرها المؤسسات المالية التي تصدر هذه البطاقات، فإنه أيضًا تتوافر خدمة التعامل بالبطاقة مباشرة في الحياة الاقتصادية من خلال رقم البطاقة.

وقد امتد نشاط بطاقات الائتمان إلى شبكة الإنترنت، فانفتح المجال لها لكي تضع عملية استخدامها في محك على درجة عالية من الخطورة إزاء مظاهر الاحتيال التي يتم بها الاستيلاء على كروت الائتمان.

فالاستيلاء على بطاقات الائتمان عبر شبكة الإنترنت أمر ليس بالصعوبة بمكان إطلاقا، فلصوص بطاقات الائتمان مثلا يستطيعون سرقة مئات الألوف من أرقام البطاقات في لحظات من خلال شبكة الإنترنت، ومن ثم بيع هذه المعلومات لآخرين.

وأثبتت شبكة (MSNBC) عمليًا سهولة الحصول على أرقام بطاقات الائتمان من شبكة الإنترنت، حيث قامت بعرض قوائم تحتوي على أكثر من (2500) رقم بطاقة ائتمان حصلت عليها من سبعة مواقع للتجارة الإلكترونية باستخدام قواعد بيانات متوفرة تجاريًا، ولم يكن يصعب على أي متطفل استخدام هذه الوسيلة البدائية للاستيلاء على أرقام تلك البطاقات

= عليه هذا الاسم نسبة إلى القانون الذي يحمل هذا الرقم في دولة نيجيريا والذي يجرّم الحصول على أموال الغير بطرق الاحتيال، والذي ظهر في بداية الثمانينيات حينما تعرضت نيجيريا لموجة من التضخم أدت إلى زيادة نسبة البطالة، وتوجّه كثير من الشباب المؤهلين تقنيًا إلى ابتكار وسائل احتيال تطورت لتصبح من خلال الإنترنت، ثم انتقلت الظاهرة إلى دول إفريقية ثم آسيوية وأوروبية.
http://www.uaeec.com/news-action-show-id-18787.htm

واستخدامها في عمليات شراء يدفع قيمتها أصحابها الحقيقيون.[1]

وعلى الرغم من أن الاستيلاء على كروت الائتمان عبر شبكة الإنترنت يكون بغرض الحصول على سلع وخدمات يتم سداد مقابلها المادي من كروت الائتمان المختلسة، إلا أن البعض يرى أن موضوع اختلاس كروت الائتمان لا يشكل سرقة مادية أساسًا، وإنما يكون عدوانًا على الائتمان تحديدًا باستغلال قيمة الضمان من قِبَل من ليس له الحق فيه[2]، إذ إن المال المضمون بالائتمان لم تخرج حيازته ماديًا على وجه التحديد، وإنما كل ما في الأمر أنه يتم إنفاقه لصالح الغير ممن لا يجوز له إنفاقه دون إرادة صاحبه، وعليه فنقطة التفاعل في الائتمان هي مسألة الإنفاق ومدى جوازه، وليس الحيازة المادية كما في جريمة السرقة.

كما أثيرت إشكالية أخرى حول أرقام بطاقات الائتمان عبر شبكة الإنترنت، والتكييف القانوني حول الاستيلاء غير المشروع عليها، فقد قال البعض بعدم توافر جريمة السرقة على اعتبار أن ما تمت سرقته عبر شبكة الإنترنت ليس هو كارت الائتمان، وذلك لعدم توافر الوسيلة المادية، وإنما

(1) يقترح بعض الخبراء استخدام بطاقة ائتمان خاصة بالإنترنت يكون حدها الائتماني معقولا، بحيث يقلل من مخاطر فقدانها والاستيلاء غير المشروع عليها، وهو الأمر الذي بدأت بعض البنوك الدولية والمحلية في تطبيقه أخيرًا، كما يقترح وجوب تغيير نظام الشراء عن طريق شبكة الإنترنت، وعدم الاكتفاء برقم البطاقة الائتمانية فقط، بل يجب أن تكون هناك مطالب أخرى، مثل ضرورة أن تطلب بيانات عن العميل كرقم تحقيق الشخصية والعنوان والتوقيع المعتمد في البطاقة، ويجب إدخال رقم (كودي) خاص بالعميل؛ حتى لا يستغل التقاط أرقام بطاقات ائتمان لبعض العملاء من الشبكة وإعادة التعامل بها دون علم أصحابها.

(2) د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان، مرجع سابق، ص 5.

فقط كود الكارت؛ لذلك يطلق على هذه الجريمة أحيانًا مصطلح " سرقة الهيئة ".

وعلى الرغم من أن اتجاهًا فنيًا يذهب إلى أن الحيازة غير المشروعة لأرقام كروت الائتمان التي تتم عبر شبكة الإنترنت إنما هي على درجة كبيرة من الصعوبة كعملية تقنية تحتاج إلى برمجة معقدة، وبالتالي تعد حركة الحيازة المادية لها أسهل بكثير من حيازتها عبر شبكة الإنترنت، على الرغم من ذلك فإن حالات اختلاس هذه الأرقام عبر شبكة الإنترنت من الخطورة بمكان، وهو ما دفع المشرع الفيدرالي الأمريكي إلى اعتبارها جريمة بعد تزايد حالات ضبطها، ومنها في عام 1996 تم ضبط حاسوب محمول "Laptop"، يحتوي على 341.000 رقم لكروت ائتمان تخص أحد المكاتب التابعة لمؤسسة ".Visa card tin" في كاليفورنيا، وفي عام 1997 قام أحد علماء جامعة سان فرانسيسكو باستخدام حاسوب في الجامعة واختلاس أسماء مالكي أرقام عدد 100.000 كارت ائتمان، وكذلك بيانات أخرى من خلال اختراقه لمجموعة مزودي خدمات إنترنت، وقام بوضعها على أسطوانة مضغوطة، ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار، ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة، وحوكم مرتكبها وعوقب بالسجن ثلاثين شهرًا.[1]

وفي إمارة دبي بدولة الإمارات العربية المتحدة في أواخر عام 2001 قام مهندس حاسبات آسيوي يبلغ من العمر 31 عامًا بالعديد من السرقات

(1) د. بلال عبد المطلب بدوي، البنوك الإلكترونية، البنوك الإلكترونية ماهيتها, معاملاتها, المشاكل التي تثيرها, مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون, كلية الشريعة والقانون وغرفة تجارة وصناعة دبي, 10: 12 مايو 2003, إدارة المطبوعات، جامعة الإمارات, المجلد الخامس، ص67.

المالية من حسابات عملاء في 13 بنكًا محليًا وعالميًا حيث قام باختلاس الأموال من الحسابات الشخصية وتحويل تلك الأموال إلى حسابات وهمية قام هو بتخليقها، كما قام أيضًا بشراء العديد من السلع والخدمات عبر شبكة الإنترنت مستخدمًا بيانات بطاقات الائتمان والحسابات الشخصية لعدد كبير من الضحايا، كل ذلك تم من خلال الدخول للشبكة من خلال أحد مقاهي شبكة الإنترنت العامة المنتشرة في دبي، وقد بلغت قيمة الاختلاسات حوالي 300 ألف درهم من البنوك المحلية بالإمارات فقط .[1]

الفرع الثاني

تأمين وسائل الدفع الإلكتروني

تتم عملية الدفع الإلكتروني[2] من خلال ثلاثة أطراف: العميل المشتري، والتاجر البائع، والبنك الذي يدير الوسيلة التي يتم الدفع أو الوفاء بواسطتها، ويرجع المتعاملون إلى الدفع الإلكتروني كوسيلة

(1) وكذلك قام شخص ألماني بالدخول غير المشروع إلى أحد مزودي الخدمات واستولى على أرقام بطاقات ائتمانية خاصة بالمشتركين، ومن ثم هدد مزود الخدمة بإفشاء أرقام تلك البطاقات ما لم يستلم فدية، وقد تمكنت الشرطة الألمانية من إلقاء القبض عليه.

(2) نص القانون العربي الاسترشادي للتجارة الإلكترونية على أن يتمّ الوفاء بأثمان السلع والخدمات التي تمْ تنفيذها طبقًا للعقود الواردة في هذا القانون بإحدى وسائل أو أدوات الدفع الإلكتروني. وذكر وسائل الدفع الإلكتروني على سبيل المثال وهي:

- بطاقات الوفاء الإلكترونية.
- التحويل الإلكتروني للأموال.
- النقود الإلكترونية.
- الاعتماد المستندي الإلكتروني.
- أي وسيلة من وسائل الدفع الإلكتروني الأخرى.

لتسوية المديونيات التي تنشأ عن تصرفات قانونية تبرم بينهم بطريقة إلكترونية، ويلزم تأمين هذه العملية تأمينًا قانونيًا[1] لمصلحة التاجر، والدائن، والعميل المشتري بطريقة تجنبهم أية مخاطر.

أولا: التأمين القانوني لعملية الدفع من جهة التاجر البائع:

يجب أن تكون عملية الدفع الإلكتروني مؤمنة لمصلحة التاجر القابض في عملية الوفاء، ولبلوغ هذا الهدف يجب أن تكون وسيلة الدفع المستخدمة، ومشمولة بضمانات تضمن للتاجر حصوله على الثمن كاملا دون أن يتحمل مخاطر عدم ملاءة المشتري، مع ضمان عدم اعتراض مصدر الأمر بالوفاء على العملية.

ويتضمن الوفاء بالنقود الإلكترونية عدم إمكانية الرجوع في الأمر بالدفع، وفقا لما نص عليه الكثير من المشرعين وعلى رأسهم المشرع الفرنسي الذي نص صراحة بعدم جواز الرجوع أو سحب الأمر بالدفع بعد صدوره، وذلك خلافًا لما استقر عليه القضاء الفرنسي من أن الاتفاق على عدم الرجوع لا يمنعه، ولا يكون لهذا الاتفاق من أثر سوى تحريك مسئولية المخل بالتزام تعاقدي.

ويستلزم تأمين التاجر الدائن منع الرجوع في الأمر بالدفع بعد

(1) وتجب الإشارة هنا إلى أن التأمين القانوني يرتكز على التأمين الفني.

CAPRIOLI Eric A, Préuve et signature dans le commerce electronique, Droit & Patrimoin, n 55, December, 1997 , p. 57.

والحقيقة أننا نساير الرأي الذي يرى صحة هذا الأمر, بمعنى أنه كلما كان التأمين الفني محكمًا كلما كان التأمين القانوني سهلا, فمثلا عند تأمين التوقيع الإلكتروني من الناحية الفنية يمنع الغير من تزويره, وهذا يسهل التأكد من صدور التوقيع الإلكتروني من الشخص الذي يجب صدوره منه, الأمر الذي يبعث الطمأنينة في قلب المحكمة ويدفعها بالتالي إلى الاعتراف به.

صدوره، ولكن هذا المنع يجب ألا يكون مطلقًا، وإنما يلزم أن يستثنى منه حالات الرجوع المستندة على أسباب ترتبط بصحة الوفاء كتصرف قانوني، ومثال ذلك الدفع المبني على أمر صادر من سارق كارت الوفاء أو ممن وجده بعد فقده، ولا يعد الأمر هنا رجوعًا عن الأمر بالدفع، إذ إن الرجوع لا يبحث ولا يتصور إلا في الحالات التي يكون فيها الأمر بالدفع صادرًا ممن له الحق قانونًا في إصداره[1].

ويجب إحاطة عملية الدفع بضمانات لصالح التاجر تجعله بمنأى عن خطر إعسار أو عدم ملاءة، فلا يصح ولا يجوز أن يقوم التاجر بتسليم البضاعة، ثم يكتشف بعد ذلك عدم وجود رصيد في حساب العميل، وتلعب الضمانات الدولية المستقلة المسماة بخطابات الضمان دورًا مهمًّا في هذا الصدد، وخاصة في تسوية المعاملات الإلكترونية مرتفعة القيمة؛ إذ إن الرجوع إلى الضمان المستقل كتعهد مباشر من جانب مصدر الخطاب لمصلحة المستفيد بناءً على طلب العميل الآمر لم يعد مقصورًا على عقد دون عقد، بل أصبح من الممكن استخدامه في تسوية المعاملات الناشئة عن العقود الإلكترونية، وهنا يستطيع التاجر أن يطلب تسييل الخطاب في حالة تقاعس المشتري عن دفع الثمن، وذلك بموجب التزام البنك في مواجهته التزامًا مستقلا عن علاقة العميل بالبنك.

كما يمكن أن تلعب الكفالة المصرفية هي الأخرى دورًا مهمًّا في هذا الصدد، لما تتضمنه من تعهد البنك في مواجهة الغير بتأدية ما يشغل ذمة عميله تجاه هذا الغير، وذلك إذا تقاعس العميل عن الوفاء بهذا الالتزام،

(1) ESPAGNON Michel, La securité des Paiements effectues sur des reseaux ouverts (internet) , Problematique juridique generale, in Colloque sur , Les novelles pratiques delictuelles liées aux technologies de la communication, Poitiers les 22 et 23 november 1996, Presses universitaires de France, 1999, p. 112.

وبذلك يكون أمام التاجر مدينان يستطيع أن يرجع على أحدهما إذا تقاعس المدين الآخر، وتجب الملاحظة أن ثمة فارقًا بين التزام البنك في خطاب الضمان، والتزام الكفيل في الكفالة، فالضمان في خطاب الضمان يتخذ شكل تعهد مباشر من البنك للغير دائن العميل ومستقل عن علاقة أي منهما بهذا العميل، فالبنك هنا لا يتعهد بضمان تنفيذ التزام عملية إذا تقاعس هذا الأخير عن القيام بالتنفيذ، كما هو شأن الكفيل في الكفالة، بل يتعهد بدفع مبلغ نقدي معين أو قابل للتعيين، وذلك أيًا كانت طبيعة التزام العميل أو مقدار مديونيته، وبغض النظر عن أية معارضة قد تأتي من جانب هذا الأخير.[1]

وتأمين عملية الدفع الإلكتروني بالنسبة للتاجر لن تكون فعالة إلا بإقامة نظام قوي وجيد للإثبات، نظام إثبات لا يتم الاعتراف بموجبه فقط بالمستندات الإلكترونية، وإنما أيضًا الاعتراف بحجية للتوقيع الإلكتروني تضاهي قوة الحجية المعترف بها للتوقيع التقليدي اليدوي، وهذا ما فعله أغلب المشرعين وفي مقدمتهم المشرع الفرنسي والمشرع الأمريكي والمشرع الإماراتي والمشرع المصري، والقانون النموذجي بشأن التوقيع الإلكتروني الذي أعدته لجنة قانون التجارة الدولية التابعة للأمم المتحدة.

وفي الدول التي لم تعترف بعد بالتعادل الوظيفي بين المستندات المكتوبة والمستندات الإلكترونية من ناحية، وبين التوقيع اليدوي والتوقيع الإلكتروني من ناحية أخرى، فيمكن التغلب على هذه المشكلة من خلال استغلال المرونة التي تبديها التشريعات المختلفة في هذا المجال،

(1) د. بضراني نجاة، الائتمان المصرفي بطريق التوقيع (الاعتماد بالقبول، الكفالة المصرفية، خطاب الضمان)، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1987، ص 273 ، وما بعدها.

وتتجسد هذه المرونة في عدم تعلق قواعد الإثبات بالنظام العام، ومن ثم يجوز للأطراف الاتفاق على مخالفتها، بالاتفاق مثلا على أن التصرف الذي تتعدى قيمته نصاب الإثبات بالكتابة يمكن إثباته بشهادة الشهود أو البينة أو القرائن.

ومن جانب آخر نجد معظم التشريعات وخصوصًا تلك التي تنتمي إلى العائلة اللاتينية، تقرر مبدأ حرية الإثبات في المواد التجارية دون تقيد بقواعد الإثبات المدني، فيجوز إثبات الثابت بالكتابة بغير الكتابة، كما أنه يجوز إثبات التصرفات القانونية التجارية مهما بلغت قيمتها عن طريق شهادة الشهود أو القرائن وغيرها من طرق الإثبات.[1]

ومن جانب القضاء أكدت محكمة النقض الفرنسية ومحكمة النقض المصرية, والمحكمة الاتحادية العليا بدولة الإمارات, ومحكمة تمييز دبي, على جواز اتفاق الأطراف على مخالفة قواعد الإثبات، وقررت صحة مثل هذه الاتفاقيات[2]، كما قررت أن قواعد الإثبات ليست من

(1) انظر المادة 69 من القانون التجاري المصري الجديد والتي تنص على أنه: "يجوز إثبات الالتزامات التجارية أيا كانت قيمتها بكافة طرق الإثبات، ما لم ينص القانون على غير ذلك ". وفي فرنسا انظر نص المادة 109 من القانون رقم 80 ـ 525 بشأن إثبات التصرفات القانونية والصادر في 1980/7/12, وكذلك نص المادة 1341 من القانون المدني الفرنسي. وفي هذا الصدد يذهب رأي من الفقه الفرنسي. إلى أن الشرائط الممغنطة التي تسجل عليها الأصوات والمعلومات في الحاسبات الإلكترونية وإن كانت لا تعد وسيلة من وسائل الإثبات بالكتابة وفقا لنص المادة 1341 من القانون المدني الفرنسي. إلا أن المحاكم يمكن أن تأخذها كقرينة تعكس وجود اتفاق قد أبرم بين الطرفين, انظر:

YVES GUYON, Droit des affaires, TI: Droit commercial general et societés, 9 ed., ECONOMIA, 1996, n 78, p. 72.

(2) وقد قررت محكمة النقض الفرنسية هذا القضاء بمناسبة قضية Credicas =

النظام العام.[1]

والواقع أن الاتفاق على مخالفة قواعد الإثبات يكون من خلال شرط بين كل من التاجر البائع والعميل المشتري يتم النص عليه في العقد المبرم بينهما، ولضمان فعالية مثل هذه الاتفاقيات يجب ألا تخالف المادة 1/132 من القانون الفرنسي الصادر في أول فبراير 1995 والخاص بحماية المستهلك من الشروط التعسفية[2]، والتي من شأنها خلق نوع من عدم التوازن الواضح بين حقوق والتزامات طرفي العقد (المستهلك والبائع)، ومن الشروط التي تعد تعسفية تلك التي تؤدي إلى تحديد وسائل الإثبات المتاحة أمام المستهلك بغير مسوغ قانوني، ويذكر أن القانون الفرنسي يقرر أن مثل هذه الشروط تعد غير مكتوبة ويتم تنفيذ العقد بدونها.

= مشار إليها في:

Jerome HUET, Aspects juridiques du telepaiement, JCP, Ed. G., I, 3524, 1991, p.288.

وقد سهل هذا القضاء على الفرنسية للاتصالات وتوزيع الكهرباء تحصيل مستحقاتها بالطريق الإلكتروني، ولكن على هذه الشركات أن تنص في العقد على أن الدفع سوف يتم بطريقة إلكترونية حتى ولو جاوزت قيمة الفاتورة نصاب الإثبات بالكتابة.

(1) الطعون أرقام 1454، 1523، 1637 لسنة 60 ق، جلسة 2000/8/7، نقض جلسة 1979/12/19، س 30 ج 3، ص 324، المستحدث من المبادئ التي قررتها الدوائر التجارية بمحكمة النقض أول أكتوبر 1999 حتى 30 ديسمبر 2000، ص 4 ، الطعن رقم 772 لسنة 64 ق، جلسة 2002/12/19 ، المستحدث من المبادئ التي قررتها الدوائر المدنية بمحكمة النقض أول أكتوبر 2002 حتى سبتمبر 2003، ص 4.

(2) **ESPAGNON Michel, La securité des Paiements effectues sur des reseaux ouverts (internet) , Problematique juridique generale, in Colloqu'e sur , Les novellrs pratiques delictuelles liees aux technologies de la communication, op. cit., 1999, p. 117.**

والحقيقة أن إمكانية اتفاق الأطراف على ما يخالف قواعد الإثبات نظرًا لعدم تعلقها بالنظام العام تبقى مسألة نظرية نظرًا لصعوبة تطبيق هذا الاتفاق في البيئة الإلكترونية[1].

وإذا كان في التشريعات الداخلية قواعد يمكن تطويعها نظريًا بشكل يجعلها متلائمة وصالحة للتطبيق على إثبات الوفاء الذي يتم بالطريقة الإلكترونية، فهناك أمور تتطلب تدخلا تشريعيًا، خاصة في الدول التي لم تأخذ بعد بقواعد للإثبات تساير التطور الحديث في مجال التجارة الإلكترونية، يضفي هذا التدخل على الرسائل الإلكترونية التي تتضمن أمرًا بالوفاء من جانب المدين والمحفوظة بشكل يمكن قراءته بوسيلة إلكترونية أو المنتجة بواسطة مدخلات موجودة بالحاسب، نفس القيمة القانونية أو الحجية في الإثبات التي تكون للمستندات الورقية المكتوبة.

ثانيا: التأمين القانوني لعملية الدفع من جهة العميل المشتري أو المستهلك:

تأمين عملية الدفع بالنسبة للمشتري المستهلك تأخذ بعدين، الأول يتمثل في البحث عن وسيلة تضمن له عدم السحب من رصيده المتاح بموجب وسيلة الدفع المستخدمة إلا للمبالغ المتفق عليها كمقابل لثمن البضاعة أو مقابل الخدمة محل العقد المبرم، ويتمثل البعد الثاني في إقامة نظام يربط بين لحظة الدفع ولحظة التسليم؛ إذ إن كلا من طرفي العملية لا يرضى البدء في تنفيذ التزامه إلا إذا قام الطرف الآخر بالفعل بتنفيذ التزامه.

وإيجاد هذه الآلية التي تمنع التاجر البائع من سحب مبالغ أكثر من المتفق عليها أو غير ذلك من التصرفات التي تحدث ضررًا بالعميل، يتوقف على الأمور التالية:

(1) CAPRIOLI Eric,A P'reuve et signature dans le commerce electronique, Droit & Patrimoin op. cit., 1997, p. 58.

1) تفعيل مسئولية البنك عن أية أخطاء تقصيرية أو تعاقدية يكون من شأنها الإضرار بالعميل، مثل قيام البنك بإجراء تحويل مصرفي من حساب العميل إلى حساب التاجر دون أن يكون هناك أمر بالتحويل، أو وجود أمر غير صحيح بالتحويل، أو وجود أمر صحيح بالتحويل ويقوم البنك بتحويل المبلغ إلى شخص غير التاجر الذي حدده العميل في أمره[1]، ويجب في هذا الصدد الإقلال من الشروط التي تضعها البنوك وتعفي نفسها بموجبها من المسئولية أو تخفف منها[2].

2) يجب على البنك قبل تنفيذ أوامر الدفع الصادرة إليه، التأكد من صحة هذه الأوامر وعلى الأخص صدورها ممن له قانونًا حق إصدارها، وهذا يفرض على البنك ضرورة إجراء المطابقة بين توقيع العميل الموضوع على رسالة البيانات وبين التوقيع الذي يحتفظ به لديه.

3) عدم تحميل العميل المستهلك نتائج المخاطر المرتبطة بتشغيل النظام المعلوماتي الذي من خلاله تتم عملية الوفاء، وتجنيبه أية خصومات أو استنزال من المبالغ المقيدة في حسابه وذلك في حالة سرقة أو فقد الوسيلة التي يتم بها الوفاء الإلكتروني.

---

(1) SALAUN Anne, Les Paiements electroniques au regard de la vente á distance, Droit de l' informatique et des Telecoms, n 99\2, p. 9.

(2) هذا مع مراعاة أن المادة 2/217 من القانون المدني المصري تقرر جواز الإعفاء من المسئولية العقدية بقولها: (يجوز الاتفاق على إعفاء المدين من أية مسئولية تترتب على عدم تنفيذ التزامه التعاقدي إلا ما ينشأ عن غشه أو عن خطئه الجسيم, ومع ذلك يجوز للمدين أن يشترط عدم مسئوليته عن الغش أو الخطأ الجسيم الذي يقع من أشخاص يستخدمهم في تنفيذ التزامه).

وتجدر الإشارة هنا إلى أن التوجيه الأوروبي المنظم للعقود بالمراسلة التي تبرم بطريق إلكتروني عبر شبكة الإنترنت، يلزم الدول الأوروبية باتخاذ الإجراءات المناسبة التي تسمح للمستهلك بطلب إبطال الدفع الذي تم بطريق الغش والتدليس، وبإجراء قيود عكسية في حسابه، فبعد أن يتم قيد المبلغ المدفوع في الحساب المدين للمستهلك، يلزم إعادة قيده في الجانب الدائن[1].

وهنا تبرز مشكلة كيفية استرداد المستهلك للمبالغ التي يكون قد قام بدفعها للبائع إلى حين التسليم النهائي للشيء المبيع، وقد فرضت المادة 6\2 من التوجيه الأوروبي الخاص بالعقود التي تبرم بين غائبين على البائع التزامًا برد هذه المبالغ، وذلك إذا ما استعمل المستهلك حقه في نقض العقد أو الرجوع عنه خلال 7 أيام التالية للتسليم، والسؤال الذي يفرض نفسه في هذا الصدد: كيف نضمن للمستهلك استرداد مثل هذه المبالغ؟

وقد قيل في هذا الصدد الكثير من الحلول نذكر منها على سبيل المثال وضع المبلغ المدفوع تحت حساب التسوية النهائية في حساب لا يمكن سحبه منه إلا بعد فوات المدة التي يجوز فيها للمستهلك الرجوع عن العقد.[2]

وتفاديًا لمثل هذه المشكلات يحيط المشرع الأمريكي المستهلك بموجب القانون التجاري الموحد بضمانات يجب احترامها في كل الصفقات التجارية، ونذكر من بين هذه الضمانات إمداد المشتري بعينة من الشيء

---

(1) Directive 97\7\CE du Parlement Europeen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matiere de contrats á distance, J.O.C.E.L 144 du 4 juin 1997.

(2) انظر غير ذلك من الحلول:
SALAUN Anne, Les Paiements electroniques au regard de la vente á distance, Droit de l informatique et des Telecoms op. cit, n 99\2, p. 14.

المبيع، فإذا ما وافق عليها فإنه يتمتع بضمان ضرورة مطابقة العينة بالمنتج النهائي الذي يتم تسليمه (المادة 313/2).[1]

ولن يتحقق هدف حماية المستهلك المشتري إلا إذا بذل هو العناية اللازمة عند استعماله لوسيلة الدفع المستخدمة، إذ يجب عليه أن يتخذ كل ما من شأنه تأمين عملية الدفع وإعلام مصدر الوسيلة بأي حادث سرقة أو فقد للوسيلة، أو تصرف يداخله غش، أو يتم إبرامه بطريق الخطأ أو الغلط.

من ناحية أخرى نجد أن الاعتماد المستندي يلعب دورا مهمًا في إيجاد آلية تربط بين تنفيذ الالتزام بالتسليم والالتزام بدفع الثمن، والحقيقة أن الاعتماد المستندي يقوم بدور فعال في القضاء على عدم الثقة القائم بيم الطرفين، فالبائع لا يرضى بتسليم المبيع قبل استيفاء الثمن، كذلك حال المشتري الذي لا يوافق هو الآخر على تنفيذ التزامه بدفع الثمن إلا بعد التأكد من الحصول على المبيع.

وتقوم فكرة الاعتماد المستندي على الاستعانة بالمستندات التي تصدر بمناسبة تنفيذ عقد البيع، فيشترط البائع الإلكتروني على المشتري الإلكتروني في عقد البيع الإلكتروني الذي ينعقد بينهما من خلال شبكة الإنترنت أن يفتح له اعتمادًا من قبل بنك معين يتعهد بالوفاء بقيمة الاعتماد بمجرد تقديم البائع المستندات التي تفيد تسليم البضاعة وتتطابق مع شروط الاعتماد.

وبما أننا بصدد تسوية الديون الناشئة عن المعاملات التجارية الإلكترونية باستخدام إحدى وسائل الدفع الإلكتروني، فإن فتح الاعتماد لن

(1) **Lionel COSTES, Apercu sur le droit du commerce electronique aux Etats-Unis, Droit & Patrimoine, decembre 1997 , p. 66.**

يـتم بطريقة تقليدية، وإنما سـوف نلجأ إلى الاعتماد المستندي الإلكتروني[1].

ويجري فتح الاعتماد وسريانه بين أطرافـه الثلاثـة: البـائع (المستفيد من الاعتماد) والمشـتري (الآمر بفتح الاعتمـاد) والبنـك (فاتح الاعتماد) بطريقة إلكترونية باسـتخدام البريـد الإلكـتروني[2]، فيقوم المشتري بإرسال طلبه بفتح الاعتماد إلى البنك، فإذا ما وافق هذا الأخير على فـتح الاعـتماد يرسل إلى المـشتري مـضمون الاعتماد، وأخيرًا يقوم المستفيد بعد إخطـاره بفـتح الاعـتماد بإرسـال المستندات الخاصة بتنفيذ عملية البيـع واللازمـة لـصرف قيمـة الاعتماد إلى البنك فـاتح الاعـتماد بنفس الطريقة التي أرسل بها طلب فتح الاعتماد[3]، أي باستخدام البريـد الإلكـتروني، وبشرـط أن يـتم إرسال المستندات خلال المدة التي يبقى خلالها الاعتماد ساريًا.

وبعد أن يتلقى البنك المستندات الخاصة بالعملية، يقوم بفحـص المسـتندات بالقـدر الـلازم للتأكد من مطابقتهـا لـشروط الاعتمـاد المفتوح إلكترونيًا، فلا يتحمل البنك مسـئولية عـن شـكل المستندات أو كفايتها أو صحتها أو زيفها

(1) د. بلال عبد المطلب بدوي، البنوك الإلكترونية ماهيتها, معاملاتها, المشاكل التـي تثيرهـا, مرجـع سـابق، ص 21 وما بعدها.

(2) Olivier BERTHIER, Le credit documentaire á l heure d internet, BANQUE magazine, n 639, septembre 2002, p. 64.

(3) وفي نطاق التجارة الإلكترونية توجد بعض الأنظمة التي تيسر الإرسال الإلكتروني للمستندات التجارية التـي تكون مطلوبة عادة قبل القيام بالـدفع, مثـل نظـام البـوليرو BOLERO SYSTEM ونظـام تريـد كـارد TRADE CARD, انظر د. محمود أحمـد إبـراهيم الشرقاوي, مفهـوم الأعمـال المصرفية الإلكترونيـة واهم تطبيقاتها, بحث مقـدم إلى مـؤتمر الأعـمال المصرفية الالكترونيـة بـين الشرـيعة والقـانون، جامعـة الإمارات، كلية الشريعة والقانون، 10-12 مايو 2003, ص 25.

أو أي أثر قانوني لأي منها[1].

وإذا ما انتهى البنك إلى مطابقة المستندات لشروط الاعتماد قام بالدفع إلى البائع المستفيد من الاعتماد، والدفع قد يتم هنا عن طريق التحويل المصرفي الإلكتروني لمبلغ الاعتماد إلى حساب المستفيد، مع القيام بقيد المبلغ في الجانب المدين لحساب العميل المشتري، كما يمكن أن يتم الدفع بطريق الكمبيالة المستندية، وذلك عندما يتعهد البنك في عقد فتح الاعتماد بقبول الكمبيالات المسحوبة عليه من قبل المستفيد، وهنا يلزم أن يتم الرجوع إلى الكمبيالة الإلكترونية ما دمنا بصدد اعتماد مستندي إلكتروني، وفي الحالتين قد يقوم البنك فاتح الاعتماد بإتمام عملية التحويل أو بقبول الكمبيالة المستندية بنفسه أو بواسطة بنك آخر غالبًا ما يوجد في بلد المستفيد يقوم بتفويضه بتنفيذ الاعتماد.

هذا كله إذا وجد البنك المستندات مطابقة لشروط الاعتماد، وإلا فإنه يرفض الدفع ويقوم بإخطار المستفيد بذلك بطريقة إلكترونية.[2]

كما قد تثار بعض المشكلات القانونية التي تنشأ عن التعامل بالنقد الإلكتروني، وتتمثل في تحديد طبيعة النقود الإلكترونية سواء أكانت الواقعية أو القانونية، ومدى صلاحية النقود الإلكترونية للوفاء بالالتزامات.

ونستطيع القول بأن النقود الإلكترونية تمثل انعطافة في تاريخ التعامل الإنساني الذي بدأ بالمقايضة لينتهي إلى ترميز القيمة المالية في بيانات مخزنة إلكترونيًا، وهذا النمط يحتاج إلى النظر في المفهوم الوظيفي للنقود لا إلى ماهيتها، فالنقود رمز لقيمة مالية تقاس على أساسها قيمة السلع

(1) د. علي جمال الدين عوض, الاعتمادات المستندية, دراسة للقضاء والفقه المقارن وقواعد سنة 1983 الدولية, دار النهضة العربية, 1989, ص 267.

(2) Olivier BERTHIER, Le credit documentaire á l heure d internet, BANQUE magazine, op. cit, pp. 65 et 66.

والخدمات، وليس ضروريًا أن تكون بماهية معينة، فيمكن أن تكون ورقًا أو معدنًا أو بيانات إلكترونية.

كما أن النقود الإلكترونية تحتاج إلى اعتراف قانوني حتى يمكن عدها نقودًا بالمعنى القانوني، لكن هذا الاعتراف يجب أن يأتي في إطار تنظيم قانوني دولي؛ لأن هذه النقود ذات طبيعة دولية لا يمكن السيطرة على التعامل بها في إطار الحدود الجغرافية لدولة معينة، والحق الوارد على النقود الإلكترونية حق وارد على شيء مادي، ولا يمكن أن يكون شرط وجود الحاسوب للتعامل بها مانعًا من ذلك؛ لأن وجوب التعامل عبر شبكة إلكترونية لا ينفي ماديتها.

من ناحية أخرى فإنه يجب على المشرع الجنائي التدخل جنائيًا لتأمين بطاقات الدفع الإلكتروني، وذلك بسن تشريعات قانونية تضفي الحماية الجنائية على وسائل الدفع الإلكتروني إعمالا لمبدأ الشرعية, وتجرم بنص صريح إنشاء مواقع وهمية, أو عرض أرقام بطاقات ائتمانية للغير, أو تزويدهم ببطاقات ائتمان مزورة, وعدم ترك هذه الأفعال غير المشروعة للقواعد العامة, سواء أكانت صادرة من جانب التاجر أو العميل أو من قبل الغير.



المبحث الثاني

صور الحماية المختلفة للتجارة الإلكترونية

تشمل عبارة الحماية وضع حدودٍ معلومة ومعينة ينبغي عدم تجاوزها إزاء ظاهرة أو أكثر من الظواهر الاجتماعية الاقتصادية، فالحماية كمصطلح يفيد في دلالته الأولى أو مقصوده الأصلي أن ظاهرة معينة في إطار الواقع الاجتماعي الاقتصادي خضعت لإطار تنظيمي يتفق مع مقومات الدولة، بحيث لا تختل أو تفقد مقوماتها في الواقع الاجتماعي الاقتصادي، فالحماية تعد تعبيراً عن عملية التنظيم الطبيعي للظواهر الاجتماعية الاقتصادية، وهو يختلف عن مفهوم المصطلح في القاعدة الجنائية، فلا تقبل القاعدة الأخيرة إلا عند حدوث عدوان بعمل غير مشروع على المصلحة المحمية بما يرتب خطرًا ما، فإذا لم يتحقق هذا الفرض فإن المشرع يتدخل لإحداث تنظيم يتوافق مع النظم القائمة في الدولة[1].

ولا يمكن اعتبار التنظيم أو النظام الذي يتولاه القانون الوضعي للظواهر محققا مقاصده إلا بإيضاح الجانب الجنائي فيه، إذ لا يوجد أقوى وأشد من تدخل المشرع لفرض شكل جنائي للحماية.

إلا أنه بالإضافة لوجود الحماية الجنائية التي تجرم الأفعال التي تمثل اعتداءً على أموال هذه التجارة ووسائلها وأطرافها ونظامها بصفة عامة، وترتب عقابًا على مرتكبي هذه الأفعال، هناك أيضًا الحماية المدنية المقررة وفقًا للقواعد العامة في القانون المدني، ولكون التجارة الإلكترونية تتعلق بأكثر من جانب وجدنا أن هناك حماية توفرها التقنية التي تعتبر مصدر

(1) د. عمر أبو بكر بن يونس، الجرام الناشئة عن استخدام شبكة الإنترنت، مرجع سابق، ص123.

وأساس هذه التجارة، وحماية أخرى مصدرها النظم الاقتصادية التجارية القائمة، والتي توفر إجراءات وقائية غير متعلقة بالتجريم والعقاب، بحيث تكون بيانات هذه التجارة ومعلوماتها في مأمن من العبث بها عند تداولها إلا لمن يكون له الحق في ذلك، لأن هذه التجارة بوصفها نظام معلوماتي يخضع لأي مخاطر تخضع لها النظم المعلوماتية الأخرى[1]، وسوف ندرس في هذا المبحث الحماية وفق المطالب التالية:

المطلب الأول: الحماية التقنية للتجارة الإلكترونية

المطلب الثاني: الحماية المدنية للتجارة الإلكترونية

المطلب الثالث: الحماية الاقتصادية للتجارة الإلكترونية

المطلب الأول

الحماية التقنية للتجارة الإلكترونية

تستند التجارة الإلكترونية في حمايتها إلى الاتصال بين النظرية وبين التطبيق التقني؛ لأن النظم العلمية التقنية ليست في معزل عن فروض حماية نتاجها العلمي والتقني، بل إنها تمتلك وسائل الحماية الذاتية في حركة الصراع مع قوى الغير الذي يقوم بالاعتداء على المصلحة المحمية، وهي إذ تضطلع بذلك فإنها تقوم باستخدام التقنية والوسائل التي من ذات طبيعتها.[2]

ولكون التجارة الإلكترونية تعتمد على التقنية بصفة رئيسية (وهي نقطة الاختلاف الجوهرية بينها وبين التجارة التقليدية) فإنه يتعين توافر تقنيات ووسائل فنية لحماية مواقع التجارة الإلكترونية من الاعتداءات والأعمال

(1) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 179.

(2) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 119.

غير المشروعة عليها، ومنع الآخرين من التجول عبر مواقعها والعبث في محتوياتها مـن معلومـات وبيانات ذات قيمة لمالكها أو حائزها.

وسوف ندرس في هذا المطلب النظم العلمية التقنية (الفرع الأول)، وسياسات هذه التقنية في الحماية (الفرع الثاني)، ثـم نتطـرق إلى حمايـة التجـارة الإلكترونيـة بطريقـة التشـفير (الفـرع الثالث).

الفرع الأول

النظم العملية التقنية

تتمثل الوسائل التقنية في إعداد برمجيات للإنترنت توضع علـى الشبكة أو توضع في موقف دفاعي على الحاسوب، وليس مثل هـذا الأمر محصـورًا في التخصص وإنما يسـتطيع أي مسـتخدم تنمية مهارته ذاتيًا ثم إعداد برمجيات حمائية لشبكته، ولقد وصل الأمر لدى الـبعض إلى أن قـام بإعداد برمجيات تسمح ليس فقط بالتعرف على الحاسوب المعتـدي IP Searcher ولكـن أيضًـا بالرد الثأري المتمثل في برمجيات الثـأر عبـر شبكة الإنترنت، وهي برمجيات بالطبع محظورة وفق توجيهات أجهزة الضبط القضائي العالمية، إذ يقـوم الضـحية بتجميد حاسوب المعتدي عن طريـق إرسال جدول حواري Dialogue box فارضًا عليه الموافقة فقط على جملة مكتوبـة في الجـدول الحواري المذكور تتضمن إهانة أو غير ذلـك كـردة فعـل للعدوان أو السلوك غير المشروع، ولـيس أمام المعتدي سوى الموافقة أو إغلاق الحاسوب كلية.

ويراجع في ذلك توجيهات المباحث الفيدراليـة الأمريكيـة المنشـورة بمعرفـة المركـز الـوطني لحماية البنية التحتيـة (NIPC)، وهـو يقـع في مقـر مكتـب التحقيقـات الاتحـادي في واشـنطن العاصمة، وأنشئ من جانب وزارة

العدل ومكتب التحقيقات الاتحادي في فبراير 1998 بالمشاركة بين الحكومة والقطاع الخاص والشراكة التي تضم ممثلين من الوكالات ذات الصلة من الاتحاد والولايات والحكومات المحلية، وهو لجنة تقوم بتطوير الهياكل الأساسية الحيوية، وحماية النظم الحاسوبية من الاقتحام غير القانوني لمواقع الحكومة والقطاع الخاص[1].

ذلك أن من بين ما يقوم به المبرمجون لمصلحة مالك الصفحة أو الموقع هو إعداد حماية لموقعه Site على شبكة الإنترنت، وتبرز هذه الحماية في شكل إعداد برمجية مصاحبة أو متوائمة مع الموقع أو الصفحة، هدفها الحماية من الانتهاك أو الإساءة إليه، وتعد برمجيات بروكسي- Proxy[2]

---

(1) Highlights, National Infrastructure Protection Center, Issue 7.01 July 15, 2001.
It is a joint government and private sector partnership that includes representatives from relevant agencies of federal, state and local government. The concept evolved from recommendation of the President's Commission of Critical Infrastructure Protection and from the government's experience in dealing with illegal intrusion into government and private sector computer systems over the years

(2) البروكسي هو برنامج (Software) يتم تركيبه على أجهزة خادمة، ولذلك يسمّى مجازًا باسم خادم البروكسي، مثله في ذلك مثل خادم الويب الذي هو أيضًا عبارة عن خادم برمجي، وللبروكسي- ثلاث وظائف رئيسية: 1- التخزين:(Caching) وهذه هي الوظيفة الأساسية للبروكسي، حيث يقوم بتخزين المواقع والصفحات بحسب ما تم تخصيصه عليه، وتقديمها للمستخدم، وهذا من شأنه أن يجعل التصفح أسرع.

2- التصفية:(Filtering) وهذه العملية يقوم بها البروكسي بشكل جانبي بالإضافة للعملية الأساسية وهي الـ caching بحيث يقوم بحجز المواقع غير المرغوبة، والسماح لغيرها من الطلبات بالمرور، ومن الجدير بالذكر أن البروكسي لا يقوم بذلك بشكل أساسي، بينما يقوم برنامج من نوع Firewall بذلك بكفاءة أكبر. =

مثالا لذلك، فهي نظم تقنية مهمتها الأساسية فضلا عن كونها حواجز أمنية أو نارية أنها تستخدم كمزود أو وسيط لتسريع التعامل مع شبكة الإنترنت، وأمكن تطويرها لكي تكون عاملا تخزينيًا كبيرًا، فتقنية بروكسي تقوم ليس فقط باستحضار سريع للصفحة المطلوبة، وإنما تخزن صورة مطابقة في ذاكرتها أو قاعدة بياناتها تكون جاهزة وبسرعة أكبر عند طلبها مرة أخرى.

إن مواقع الشركات والمؤسسات والمصارف قد تكون عرضة للإساءة والانتهاك الإجرامي؛ لذلك جرت العادة على أن تتمتع تلك المواقع بالحماية للتقنية المستخدمة أو التي تستخدمها في معاملاتها، مثل البرمجيات المعدة للدفاع ضد الفيروسات Anti-virus عبر شبكة الإنترنت، وكذلك إعداد الحائط الناري Fire wall الذي يعمل كسد مانع للاختراق في تلك المواقع، وبرمجيات IP Control التي تتعرف على رقم الحاسوب المخترقIP address، باعتبارها برمجيات تعمل كمراقب بروتوكول شبكة الإنترنت لمعرفة شخصية الدخيل.

الفرع الثاني

سياسات التقنية في الحماية

تنطلق السياسة العامة للحماية العلمية التقنية من ضرورة التوصل إلى أفضل الوسائل للحد من العدوان غير المشروع المرتكب ضد التجارة الإلكترونية [1].

=3 - التحويل:(Redirection) وهو أن يقوم بتحويل بعض طلبات المواقع إلى جهات أخرى، كأن يقوم بتحويل طلبات المواقع غير اللائقة إلى مواقع جيدة مثلا.

(1) مصطفى منير السيد - جرائم استعمال السلطة الإقتصادية - رسالة دكتوراه - الهيئة المصرية العامة للكتاب- القاهرة - 1992 - ص 43.

وعلى الرغم من الامتياز العام الذي تتمتع به السياسة العلمية التقنية كوسيلة حماية عبر شبكة الإنترنت، وكونها تمثل أهم وسائل الحماية حتى الآن بما تمثله من قوة ردع قد تكون فورية باستخدام البرمجيات عبر شبكة الإنترنت، مع ما يشمل ذلك من قدرتها على اتخاذ الأسلوب الوقائي، إلا أن عملية الردع فيها تأخذ طابع الردع الخاص غير المعترف به من قبل المشرع؛ لأنها تعد محل صراع من طابع فردي يتعارض مع مفهوم الردع كما هو مقرر في القانون الجنائي، وإن كان من الممكن إدخاله في إطار الدفاع الشرعي في حالات خاصة.

وضعت السياسة العلمية قاعدة الحماية الذاتية، ومن ثم استطاعت أن تضع قاعدة التطور الذاتي للإنترنت بكل سهولة، إذ بفضل حالة اللامركزية التي عليها شبكة الإنترنت والحرية الكاملة في التعامل أمكن للراغبين الوصول إلى مرحلة الاحتراف فيها، بحيث يكون لكل مستخدم تطوير كيفية الحماية وفقًا لإمكانياته، وهو أمر جعل الإبداع فيه ممكنًا للجميع، فظهرت ميول شابة من خلالها تعد وبحق نواة تطوير، بل وأصبح التطوير لغة شبكة الإنترنت الحقيقية أو اللغة المتداولة فيها.

إن التطوير الذاتي لأساليب الحماية على شبكة الإنترنت أصبح لغة قانونية يتحدث بها فقه القانون باعتبارها عاملا متغيرًا، ولقد أفصح اتجاه في الفقه صراحة عن أهمية مواجهة التغيير التقني بضرورة التواصل القانوني به، ويسوق فقه القانون العام الكندي مثالا جيدًا على ذلك (موضوع تطوير برمجيات الحاسوب) إذ إن كل تطوير في هذه البرمجيات يستدعي تغييرًا في الوثيقة القانونية والتعليمات المصاحبة لها[1]، مثل هذه البرمجيات

(1) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 121.

امتدت فعلا إلى شبكة الإنترنت لتأخذ مكانها هناك بجدارة في المواقع والصفحات عند كل تغيير أو تطوير يحدث في الموقع أو الصفحة.

ويتعلق موضوع وضع حلول تقنية بموضوع الخصوصية Privacy، وهو من الموضوعات المعقدة جدًا، ولم يتم التوصل بعد إلى حلول حاسمة في شأنه عبر شبكة الإنترنت، لقد كانت هناك محاولة تقنية تمنح المستخدم قدرة على التحكم فيما يكشف عنه من معلومات حين إبحاره عبر الشبكة، وفقًا لنظام أمني متكامل يؤدي لحماية البيانات عبر شبكة الإنترنت، بما يعرف بالاتجاه التقني[1].

مثل هذا الاتجاه التقني يجعل منطق سياسة الحماية بالأسلوب التقني هو سيد الموقف، حيث يكون الاتجاه السائد هو الدور الوقائي الذي يجب أن تقوم به التقنية، وهو بدون شك دور خطير إلا أنه يخلق معادلة صعبة، حيث إنه سوف يساهم بشكل أو بآخر في تقوية الاتجاه الذي يقول بعدم إمكانية تنظيم شبكة الإنترنت قانونيًا، ومما يجعل النظام الوقائي الذي

---

(1) ومثال ذلك قيام الاتجاه التقني لدى الحكومة الأمريكية بعد الحادي عشر من سبتمبر 2001 على دعم برمجية (DCH10000) كارنيفور Carnivore التي تسمح بالتجسس على الشبكات والحواسيب حول العالم، كما أسقط القضاء الأمريكي في قضية Scarf طلب الدفاع بضرورة تفسير طبيعة عمل برمجية التجسس Key Logger mechanism، حيث أخذت المحكمة الابتدائية الفيدرالية لشمال جيرسي North Jercy برأي الادعاء بأن هناك برمجيات متفوقة ليس من مصلحة الأمن القومي الأمريكي الكشف عنها أو جعلها تخضع لقانون حماية إجراء المعلوماتية، بما يعني عدم إمكانية الكشف عنها حتى ولو كان هناك عدوان على التعديل الرابع للقانون الأمريكي المتعلق بحماية الحق في الخصوصية.

- مشار إليه لدى د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 122.

يفرضه القانون في موقف ضعيف هنا، حيث إن التدابير الوقائية السابقة على الجريمة لا تفرض سوى بقانون سابق عليها، وإلا تحولت إلى أدوات تعسف غير مشروعة.

الفرع الثالث

حماية التجارة الإلكترونية بالتشفير

التجارة الإلكترونية تعتمد على التقنية بصفة رئيسية، وهي ما يميزها عن التجارة التقليدية، وبالتالي يجب توافر تقنيات ووسائل فنية لحماية مواقع التجارة الإلكترونية من الاعتداءات والأعمال غير المشروعة عليها، ومنع الآخرين من التجول عبر مواقعها والعبث في محتوياتها من معلومات وبيانات ذات قيمة لمالكها أو حائزها، ومن هنا يرى المختصون ضرورة تشفير أو ترميز هذه البيانات على نحو يمنع الآخرين من الوصول إلى هذه البيانات والمعلومات وإفسادها.[1]

ويتم التشفير باستخدام أدوات أو وسائل أو أساليب لتحويل المعلومات بهدف إخفاء محتوياتها والحيلولة دون تعديلها أو استخدامها غير المشروع، بحيث يتم التأكد من أن المعلومات التي تسلمها المرسل إليه هي تلك البيانات التي قام المرسل بالتوقيع عليها، وبحيث يتأكد المرسل أيضًا أن المعلومات لم يتسلمها شخص سوى المرسل إليه الذي يستطيع باستخدام الوسائل الفنية الاطلاع على محتوى المعلومات، وبالتالي فإن التشفير يسمح بتلافي بعض المخاطر المتوقعة من استخدام الطرق الإلكترونية في المعاملات التجارية، ويؤدي إلى توفير الثقة في المعاملات الإلكترونية، كما يتم الاطلاع على

(1) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 179.

المعلومات المشفرة باستخدام ما يسمى بالمفتاح العام وهو نظام معلن للشفرة ومفتاح خاص وهو تشفير سري، ويتعين استعمال المفتاحين للتأكد من شخصية المرسل ومن قيامه بالتعبير عن إرادته.

وقد اعترف المشرع الفرنسي بالتشفير بمقتضى قانون صدر في عام 1990 سمح للمشروعات الخاصة باستخدام التشفير بعدما كان قاصرًا على المجالات العسكرية والدبلوماسية والحكومية[1]، وخفف القانون الصادر في 26 يوليو 1990 من بعض القيود المتعلقة بالتشفير، ثم وضع القرار رقم 98-101 الصادر في 24 فبراير 1998 الضوابط المتعلقة باستخدامه.[2]

وأظهرت المعاملات المالية عبر شبكة الإنترنت الحاجة لتوفير حماية للمعاملات الإلكترونية والبيانات الاسمية عن طريق شخص ثالث لا يعد من أطراف العقد ليوثق البيانات المتبادلة وبصفة خاصة التوقيع الإلكتروني، ويشهد بصحته دون أن تكون له مصلحة شخصية في هذه البيانات، وقد عرّف التوجيه الأوروبي رقم 93/1999 الصادر في 13 ديسمبر 1999 بشأن إطار أوروبي للتوقيع الإلكتروني هذا الشخص بأنه كل شخص طبيعي أو اعتباري يقدم شهادات الصحة (التوثيق) والخدمات الأخرى المتعلقة بالتوقيع الإلكتروني (مادة 11/2)، وأكد التوجيه على التزام مقدم هذه الخدمة بالقيود الواردة بالتوجيه رقم 46/95 الصادر في 24 أكتوبر 1995 في شأن حماية البيانات الشخصية (مادة 8-1) والتزامه بعدم جمع بيانات إلا من الشخص المعني أو برضاء صريح منه، وأن تتعلق هذه البيانات

(1) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 32.

(2) د. فهد بن سيف بن راشد، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، مرجع سابق، ص 91.

بالشهادة المطلوبة (مادة 8-2).

ولم يورد قانون المعاملات والتجارة الإلكترونية الإماراتي تعريفًا للتشفير، ولكنه نظم شهادات المصادقة الإلكترونية، والجهة التي تراقب خدمات التصديق (المادة 20)، وترك قرار إنشائها لمجلس الوزراء، ونص على واجبات مزود خدمات التصديق (المادة 21)، ومنها أن يتصرف وفقًا للبيانات التي يقدمها بشأن ممارسته لنشاطه، وأن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات جوهرية ذات صلة بشهادات المصادقة الإلكترونية أو مدرجة فيها طيلة سريانها، وأن يوفر وسائل يكون من المعقول الوصول إليها، وتمكن الطرف الذي يعتمد على خدماته من التأكد مما يلي:

هوية مزود خدمات التصديق.

- أن الشخص المعينة هويته في الشهادة لديه السيطرة في الوقت المعني على أداة التوقيع المشار إليها في الشهادة.
- الطريقة المستخدمة في تعيين هوية الموقع.
- وجود أية قيود على الغرض أو القيمة التي يجوز أن تستخدم من أجلها أداة التوقيع.
- ما إذا كانت أداة التوقيع صحيحة ولم تتعرض لما يثير الشبهة.
- ما إذا كان للموقع وسيلة لإعطاء إخطار بموجب هذا القانون.
- ما إذا كان هناك وسيلة مناسبة للإبلاغ عن إلغاء التوقيع.
- وأن يوفر وسيلة للموقعين تمكنهم من تقديم إخطار بأن أداة التوقيع قد تعرضت لما يثير الشبهة، وأن يضمن توفير خدمة إلغاء التوقيع يمكن استخدامها في الوقت المناسب.

- وأن يستخدم في أداء خدماته نظمًا وإجراءات وموارد بشرية جديرة بالثقة.
- وأن يكون مرخصًا من مراقب خدمات التصديق إذا كان يعمل في الدولة.

كما نظم القانون عمل مزودي خدمات التصديق (المادة 22)، واعترف بشهادات المصادقة والتوقيعات الإلكترونية الأجنبية (المادة 23).

وأنشأ قانون التجارة الإلكترونية لدوقية لوكسمبورج على سبيل المثال نظامًا لتوثيق المعاملات الإلكترونية ليكون بأيدي أطراف محايدة، سواء من الأشخاص الطبيعيين أو الأشخاص المعنوية، ويطلق على من يقوم بهذا العمل مقدم خدمة التوثيق، حيث يتولى عملية تسليم وإدارة الشهادات الموثقة، وتقديم الخدمات الأخرى المتعلقة بالتوقيع الإلكتروني (مادة 17)، وأطلق على الوزير المختص بالأمور الاقتصادية (في إطار هذا القانون) السلطة القومية للتوثيق والرقابة، ويقوم الوزير بإدارة نظام التوثيق، ويراقب مقدمي خدمة التوثيق (مادة 17) وألزم المشرع من يقدم خدمة التوثيق بتحري صحة المعطيات المقدمة (مادة 23)، وألزم القانون من يقوم بالتوثيق بسر المهنة (مادة 19)، وبعدم جمع بيانات شخصية إلا بناءً على موافقة صريحة من صاحب الشأن (مادة 20 من قانون التجارة الإلكترونية)، وأقام القانون مسئولية مقدم خدمة التوثيق عن الأضرار التي تقع نتيجة الأخطاء التي تقع منه (مادة 27).[1]

كما عرف القانون التونسي التشفير بأنه استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تحريرها أو إرسالها

(1) د. مدحت رمضان - الحماية الجنائية للتجارة الالكترونية - المرجع السابق - ص33.

غير قابلة للفهم من قبل الغير إلا عن طريقها، أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها (المادة 5/2).

وقد أجاز مشروع قانون التجارة الإلكترونية المصري تشفير البيانات المتعلقة بالمعاملات الإلكترونية (مادة 7)، وعرف التشفير بأنه تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من اطلاع الغير عليها أو من تعديلها أو تغييرها.

ويمكن إجمال ضوابط التشفير الإلكتروني كما يلي[1]:

1) تشفير البيانات والمعلومات المتداولة والتي يتم التعامل فيها من خلال الوسائط الإلكترونية هو أمر مباح من الناحية القانونية.

2) احترام سرية البيانات المشفرة والاعتراف بحق أصحابها في الخصوصية.

3) استخدام التشفير كوسيلة يعتد بها القانون في شأن تحرير البيانات والمعلومات، ويكون بواسطة الجهات المختصة، وحسبما يحدده القانون ولائحته التنفيذية.

المطلب الثاني

الحماية المدنية للتجارة الإلكترونية

تقوم فكرة الحماية المدنية على ضرورة بناء المجتمع الإنساني، وتعد هذه الحماية البداية في بناء هذا المجتمع، وتتسع الحماية لتشمل كافة أنواع الحقوق والحريات، وتتعدد وسائلها تبعًا لتعدد المذاهب القانونية، فمن فكرة القانون العام إلى فكرة القانون المدني، والقاعدة المقررة في الحماية المدنية

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 60.

أنه ليس هناك حق بدون التزام مقابل، وفي إطار التجارة الإلكترونية التي تتخذ شبكة الإنترنت وسيلة لها حاول الفقه وضع تعريف منطقي وقانوني للعلاقات المدنية يتوافق مع الحماية المدنية، ويمكن الاستناد إليه في وضع أسس هذه الحماية في تعاملها مع الاتصالات.[1]

والتجارة الإلكترونية مثل التجارة التقليدية، تخضع لذات الأحكام والقواعد إلا ما تعلق منها بالطبيعة الخاصة والذاتية لهذه التجارة بوصفها نظامًا معلوماتيًا عبر شبكة الإنترنت، ولذا فهذه التجارة لها عناصر مادية ومعنوية وأموال يجب حمايتها مدنيًا، كما هو الحال في الحماية الجنائية.[2]

وسوف ندرس في هذا المطلب الحماية المدنية للعقود الإلكترونية (الفرع الأول)، والحماية المدنية للحقوق الإلكترونية (الفرع الثاني)، والمسئوليات والالتزامات المدنية (الفرع الثالث)، ثم نتطرق لبعض الحقوق التي صادفت مشكلات في الحماية المدنية (الفرع الرابع).

الفرع الأول

الحماية المدنية للعقود الإلكترونية

العقد الإلكتروني يتطلب لانعقاده ما يتطلبه أي عقد آخر من حيث توافر الإيجاب[3] والقبول، والمحل والسبب والثمن، وجميع شروط تحديد

---

(1) Eric. J. sinord & Barak D.jolish. controlling chaos: the emerging law of privacy and speech in cyberspace.

P.9. Stanford technology law review. vol. 1 1999.
http://slr.stanford.edu/stlr/articles/99strl1/index.htm

- at http://www.msh.parist.fr/red&s/index.htm

(2) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 180.

(3) ولما كان الإيجاب الإلكتروني إيجابًا عن بعد، فهو يخضع للقواعد الخاصة بحماية=

المسئولية المتعلقة بالمتعاقدين، لكنه يختلف عن غيره من العقود كونه ينعقد دون أن يكون لطرفيه حضور مادي بمجلس العقد وقت انعقاده، حيث يكون كل طرف في مكان مختلف عن مكان الآخر، ويفصل بينهما بعد جغرافي.

ويعرف عقد التجارة الإلكترونية بأنه العقد الذي يتم إبرامه بين طرفين بوسيلة اتصال عن بعُد، ويتم تنفيذه ماديًا أو الكترونيا، ويختلف عقد التجارة الإلكترونية عن العقد التقليدي في وسيلة الإبرام والتنفيذ، ويتفقان من حيث توافر الأركان العامة، وهي الرضا المتمثل في تلاقي الإرادتين، وأن تتجه الإرادتان إلى محل معين، مع مشروعية السبب في التعاقد[1].

ويثير التعاقد الإلكتروني العديد من التحديات للنظم القانونية القائمة، من حيث كونه ينعقد رغم البعد الجغرافي بين طرفيه، بمعنى أن الطرفين لا يجمعهما مجلس العقد، وإنما يجمعهما مجلس عقد حكمي، لكون التعاقد الإلكتروني عبر شبكة الإنترنت يلغي الحواجز المادية المعروفة[2] بخلاف

= المستهلك في العقود المبرمة عن بعد، والتي تفرض على المهني أو المورد مجموعة من القيود والواجبات التي يلتزم بها تجاه المستهلك الإلكتروني، والتي منها: تزويد المستهلك بمعلومات حول شخصية التاجر وعنوانه والمركز الرئيسي له، وعنوان البريد الإلكتروني، والخصائص الأساسية للمنتجات والخدمات المعروضة، وأوصافها، وأثمانها، ووسائل الدفع أو السداد، وطريقة التسليم، وخيار المستهلك في الرجوع في التعاقد، وإعادة إخطار المستهلك، وخدمة ما بعد البيع، ومدة الضمان، وهي الالتزامات التي أشار إليها التوجيه الأوروبي رقم (97/7) في شأن حماية المستهلك في العقود عن بعد.

(1) د. طاهر شوقي مؤمن، عقد البيع الإلكتروني، مرجع سابق، ص 23.

(2) voir: project de la loi fedrale sur le commerce electronique suisse. Jan. 201، de la assemble generale Suisse: art. 4، at. 2: les contrats conclus par telephone ou par un autre moyen de communication electronique sont censes faits.persents. si le parlis ou leures mandataires no A ete personnellement en communication.

الشأن في الحضور المادي للعاقدين في العقد التقليدي، واستهلاك الوقت فيه أثناء تبادلهما الاطلاع على نسخ مطبوعة من العقد pre-printed forms وهو ما يعرف بمصطلح معركة النماذج The battle of the forms[1].

فالعقود الإلكترونية عبر شبكة الإنترنت لا تمثل وفقًا للنظرية التقليدية عقودًا بالمعنى الصحيح، بل إنها لا تعدو أن تكون في الحقيقة سوى تعليمات Instructions أواتفاقيات Agreements ينبغي الإذعان لها، وهو الأمر الذي قرره القضاء الأمريكي في قضية America Network v. Access America[2].

ويضيف أنصار المنهج التقليدي إلى ذلك مساوئ أخرى تتعلق بالعقود المعدة على نماذج جاهزة، خصوصًا في موضوع الإرادة ومسألة الرضا، والتي تعد من الموضوعات الشائكة حين التعامل مع التكنولوجيا المتطورة أو من خلالها، حتى في ظل الاتجاه الذي يستند إلى تشريع تنظيم الاتصالات الفرنسي رقم 659-9 المؤرخ 1996/7/29[3].

وهناك اتجاه برز يعتبر أن العقود عبر شبكة الإنترنت سوف تجعل القبول acceptance في العقود يصبح إجراءً شكليًا في الواقع المادي، ويذهب هذا الاتجاه إلى اعتبار عقود التجارة الإلكترونية عقودًا رقمية، وهي

(1) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 123.

(2) American Network, Inc. v. Access America/Connect Atlanta, Inc. (SDNY،Decided، August 13, 1997) at:
http://www.ipcounselors.com/19970922.htm#a3

(3) thelen reid &priest LLP،current legal issues facing business on the internet: legal risks and how they can be avoided p.3 available online at:
http://libraary.lp.Findlaw.com/scripts/getfile.pl?FILE=firms/thelen/thelen/trp00003

بذلك تعد من العقود المسماة.

ويمكن أن يكون تأسيس العقد الرقمي صحيحًا إذا استند إلى المدلول الرقمي والاتصالات في الوقت الذي تتكامل له أركانه في القانون، لذلك يعتمد العقد الرقمي عبر شبكة الإنترنت على وجود الوثيقة المثبتة للعقد في شكل رقمي سواء باستخدام أسلوب المستند document عبر معالج الكلمات وورد word أو بلغة HTML أو لغة الملفات الإلكترونية المؤمنة (portable document format -PDF)، كل ذلك عبر شبكة الإنترنت، بمعنى أن وثيقته عبر شبكة الإنترنت عبارة عن BITS&BYTES (وحدات الوزن أو الأحجام في العالم الرقمي والحاسوب).

وبالتالي فإن ظهور العقد افتراضيًا يختلف عن الظهور المادي له، وتكون نسخته المطبوعة من الحاسوب طبق الأصل إذا توافقت مع الشكل اللازم لاعتبارها كذلك، وبالتالي تعد عقودًا أشكال الاتفاقيات المعروفة باتفاقيات EDI وهي اتفاقيات طورتها الأمم المتحدة.

ويثير موضوع النسخة الأصلية والنسخة المطابقة في مجال شبكة الإنترنت تخلف مبدأ الشكلية في العقود وفق ما هو مقرر في القانون المدني، حيث إن نية التعاقد تتفوق على الكتابة، ومثل هذا الاتجاه جعل العديد من الدول تهتم في مجال العقود عبر شبكة الإنترنت بموضوع التوقيع الإلكتروني تحديدًا لكونه تعبيرًا كاملا في العالم الرقمي عن صحة العقد، ويمكن من خلاله تعويض النقص المادي لعقود شبكة الإنترنت المتمثل في استكمال الشكلية المادية (التسجيل وإشهار العقد وحفظه مثلا)[1].

---

(1) **Thelen Reid & priest LLP، current legal issues facing business on the internet: legal risks and how they can be avoided op cit p.4.**

وتخضع القاعدة العامة للتعاقد عبر شبكة الإنترنت لمدلول التعاقد عن بعد، التي اعترف بها التوجيه الأوروبي في سنة 1997، وأتم المشرع الفرنسي الاعتراف بها في التشريع الداخلي بمقتضى الأمر المؤرخ 2001/8/23 والذي تضمن تعديلا في قانون الاستهلاك حيث تقرر تعديل المادة (16-121) منه والتي تضمنت تعريفًا للعقد عن بعد، مما أدى إلى ظهور الحاجة لحفظ وتوثيق وتخزين هذه البيانات والمعلومات المتبادلة في التجارة الإلكترونية، الأمر الذي استلزم ظهور السجل الإلكتروني كأداة للتوثيق، ومن ثم حماية التجارة الإلكترونية.

والسجل الإلكتروني يمكن تشبيهه بالدفاتر التجارية التي يلتزم التجار بإمساكها لبيان معاملاتهم التجارية، وتشترط الاتفاقيات الدولية والتشريعات الوطنية للتجارة الإلكترونية وجود سجل إلكتروني لإثبات المعاملات التجارية، فقد نص التوجيه الأوروبي الصادر سنة 2000 بشأن التجارة الإلكترونية في المادة (1/10) على أن: " الشخص الذي يعرض منتجات وخدمات من خلال نظم معلومات يمكن للجمهور الوصول إليها يلزم بأن يوفر وسائل لتخزين أو طباعة العقد ".

وعرّف القانون الإماراتي رقم 1 لسنة 2006[1] السجل الإلكتروني في

---

(1) القانون الاتحادي رقم 1 لسنة 2006 في شأن المعاملات والتجارة الإلكترونية الصادر بتاريخ 30 يناير 2006 بدولة الإمارات العربية المتحدة.
كما نص بخصوص السجل الالكتروني يعد محميا: (إذا تم بطريقة صحيحة تطبيق إجراءات توثيق محكمة، منصوص عليها في القانون أو معقولة تجاريًا ومتفق عليها بين الطرفين، على سجل إلكتروني للتحقق من أنه لم يتم تغييره منذ وقت معين من الزمن، فإن هذا السجل يعامل كسجل إلكتروني محمي منذ ذلك الوقت إلى الوقت الذي تم فيه التحقق).
وفي تطبيق أحكام هذه المادة والمادة (17) من هذا القانون في مجال تقرير ما =

المادة رقم (1) بأنه: "سجل أو مستند إلكتروني يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس، أو على وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه ".

وقد عرف القانون الأردني للمعاملات الإلكترونية في المادة (2) منه السجل الإلكتروني بأنه: " القيد أو العقد أو رسالة المعلومات التي يتم إنشاؤها أو إرسالها أو تسلمها أو تخزينها بوسائل إلكترونية "[1].

وعلى الرغم من أن القانون التونسي للمبادلات والتجارة الإلكترونية لم ينص صراحة على تعريف السجل الإلكتروني إلا أن نص المادة (14) أوجب على كل شخص طبيعي مختص بخدمة المصادقة والتوثيق الإلكترونية الإمساك بسجل إلكتروني، خاص بشهادات المصادقة على ذمة المستعملين مفتوحًا للاطلاع إلكترونيًا بصفة مستمرة على المعلومات المدونة به، كما ألزم كل مزود بخدمات مصادقة إلكترونية بحماية هذا

= إذا كانت إجراءات التوثيق المحكمة معقولة تجاريًا، ينظر لتلك الإجراءات في الظروف التجارية وقت استخدامها بما في ذلك:
(أ) طبيعة المعاملة.
(ب) خبرة ومهارة الأطراف.
(ج) حجم المعاملات المماثلة التي قام بها أي من الطرفين أو كلاهما.
(د) وجود إجراءات بديلة وتكلفتها.
(هـ) الإجراءات المستخدمة عمومًا في أنواع مماثلة من المعاملات.

(1) نشر هذا القانون في الجريدة الرسمية الأردنية في العدد رقم 4534 بتاريخ 31 /12 /2001، ويتكون هذا القانون من 41 مادة، تناولت بيان ماهية المعاملات الإلكترونية، والعقد الإلكتروني، والسندات الإلكترونية القابلة للتحويل، وتوثيق السجل، والتوقيع الإلكتروني.

السجل الإلكتروني من كل تغيير أو تحريف غير مرخص به [1].

وقد وضع قانون المعاملات البحريني لسنة 2002 تعريفًا للسجل الإلكتروني بأنه: "السجل الذي يتم إنشاؤه أو إرساله أو تسلمه أو بثه أو حفظه بوسيلة إلكترونية" كما عرف وسيط الشبكة فيما يتعلق بالسجل الإلكتروني بأنه الشخص الذي يقوم نيابة عن شخص آخر بإرسال أو تسلم أو بث أو حفظ السجل الإلكتروني، أو يقوم بتقديم أية خدمات أخرى بشأن هذا السجل. (المادة الأولى المخصصة للتعريفات).

وفي كندا عرف القانون الموحد للإثبات الإلكتروني السجل الإلكتروني بأنه " البيانات التي يتم تسجيلها أو تخزينها على وسائط أو بواسطة نظام كمبيوتر أو أية وسيلة مشابهة، وتشمل البيانات المقروءة أو المخرجات الكمبيوترية المطبوعة أو أي مخرجات أخرى من هذه البيانات "[2].

وتزداد أهمية السجل الإلكتروني كوسيلة لحماية العقد، خصوصًا أن التبادل الإلكتروني للبيانات من الممكن أن يتم في ظل عدم وجود اتفاق مسبق بين الأطراف، لذا كان من الضروري إنشاء سجلات تجارية إلكترونية لحفظ الرسائل والبيانات المتبادلة بين أطراف التعاقد، على أن

---

(1) وافق مجلس النواب التونسي على هذا القانون في 27 يوليو 2000 وصدر في 9 أغسطس 2000 ونشر في جريدة الرائد الرسمية للجمهورية التونسية في 11 أغسطس 2000.

(2) Electronic record " means data that is recorded or stored on any medium in or by a computer system or other similar device < that can be read or perceived by a person op a computer system or other similar device < it include a display , printout, or other output of that data , other than a printout referred to in sub، section 4/2.
Alan M Gahtan, Electronic Evidence, Thomas Canada Limited 1999 p 157

يكون لكل طرف في العملية التجارية السجل الخاص به[1].

وقد يثور تساؤل في موضوع العقود الإلكترونية حينما يرغب العميل في مجرد الاستعلام عن نوع معين من البضائع أو الخدمات المعروضة على شبكة الإنترنت، أو مجرد البدء في التفاوض بشأن إبرام عقد معين، ولكن يفاجأ بأن التاجر أو المهني قد أرسل إليه هذه المنتجات دون أن يطلبها على الإطلاق، الأمر الذي يثير مشكلة اعتبار مثل هذا الإرسال إيجابًا أم مجرد دعوة للتعامل أو التفاوض، وما هو تصرف المستهلك تجاه تلك المنتجات؟

وفي هذا الشأن نصت المادة (14) من توجيهات المجلس الأوروبي على أنه على الدول الأعضاء في المجلس الأوروبي أن تتخذ الإجراءات المناسبة لمنع هذه الطرق الخاصة بإرسال البضائع والخدمات إلى المستهلك دون سبق موافقته أو طلبها، واعتبار أن عدم رد المستهلك لا يعني الموافقة على قبوله هذه المنتجات.

أما قانون المعاملات الإلكترونية التونسي لعام 2000 فقد نص في المادة (26) على أنه يحظر على البائع تسليم منتج مشروط بطلب دفع لم تصدر بشأنه طلبية من قبل المستهلك الإلكتروني، وأضاف أنه في حالة تسليم منتج إلى المستهلك لم تصدر بشأنه طلبية لا يمكن مطالبة هذا الأخير بسعره أو نفقات الشحن والتسليم.

وعليه فإنه في حالة البضائع والخدمات المعروضة عبر شبكة الإنترنت والتي أرسلت للمستهلك دون أن يطلبها على الإطلاق، أي لم يتم التعاقد بشأنها مع المستهلك، فإنه يجب لتحديد إذا كان مثل هذا الإرسال يعتبر

---

(1) Bernard D. Reams. JR, Electronic Contracting Law،EDI and Business Transaction , Clark borad man callagham , 1997 p32.

إيجابًا أم مجرد دعوة للتفاوض أن يعتد بالظروف المحيطة بعملية الإرسال، وعما إذا كانت هناك معاملات سابقة بين الطرفين من عدمه, وفقا لما استقر عليه القضاء المقارن.

وحيث إن العقد يشترط الإيجاب والقبول، فإن الإيجاب الإلكتروني المتطلب في عقود التجارة الإلكترونية يكون في الغالب إيجابًا دوليًا يتم باستخدام وسائط إلكترونية وعبر شبكة دولية للاتصالات والمعلومات، لذلك فهو لا يتقيد بحدود الدول السياسية والجغرافية، ويكون الإيجاب الإلكتروني تبعًا لذلك إيجابًا دوليًا نظرًا لما تتسم به شبكة الإنترنت من الانفتاح والعالمية، ورغم ذلك فإنه لا يوجد ما يحول دون قصر الإيجاب الإلكتروني على منطقة جغرافية محددة، بحيث يكون له نطاق جغرافي ومكاني معين، أي أن الإيجاب الإلكتروني قد يكون إقليميًا أو دوليًا، ومن ثم فإن على الموجب أن يلتزم بعدم إبرام عقود أو تسليم منتجات خارج النطاق الإقليمي الذي حدده سلفًا.

أما بالنسبة للقبول الإلكتروني فلا يشترط أن يصدر في شكل خاص أو وضع معين، فيصح أن يصدر عبر وسائط إلكترونية أو من خلال الطرق التقليدية للقبول، وذلك ما لم يكن الموجب قد اشترط أن يصدر القبول في شكل معين، فعلى سبيل المثال إذا اشترط التاجر الإلكتروني في عقد البيع أن يكون القبول عن طريق البريد الإلكتروني أو عن طريق ملء الاستمارة الإلكترونية المعدة سلفًا والمبينة على الموقع، فإذا أرسل المستهلك قبوله في شكل آخر، كأن يرسله بالبريد التقليدي أو بالفاكس أو بالاتصال تليفونيًا، فإن هذا القبول لا يكون صحيحًا ولا ينعقد به العقد، ومن التشريعات التي اشترطت تقديم القبول بنفس طريقة وصول الإيجاب القانون التجاري الأمريكي الموحد Uniform Commercial Code (UCC) حيث جاء

نص المادة (2/206) على أن "التعبير عن الإرادة في القبـول يـتم بـذات طريقـة عـرض الإيجـاب". وبالتالي فإذا أرسل الإيجاب عن طريق البريد الإلكتروني أو عبر موقع الويب فيجب على القابل إن قبل التعاقد أن يعبر عن القبول بالطريقة ذاتها.

وبالنسبة لوسائل التعاقد الإلكتروني فتختلف بحسب درجة استخدام الكمبيوتر في التعاقـد، وبحسب إذا كان التعاقد بالكامل بواسطة الكمبيوتر، أم يوجد في جزء منـه عنصرـ آدمـي، وكلـما زادت درجة استخدام الكمبيوتر في هذا المجال فإننا نتحرك بعيدًا عن القواعـد التقليديـة، ونجـد أنفسنا أمام قواعد خاصة بالتعاقد الإلكتروني.

والتعاقد عن طريق الوكيل الإلكتروني أو التعاقـد عـن طريـق الوسـائط الإلكترونيـة المؤتمتـة يأخذ ثلاثة أشكال:

1) من إنسان إلى كمبيوتر وبالعكس: أي تعاقـد مـا بـين الوسـيط الإلكـتروني[1] المـبرمج وبـين شخص طبيعي، وذلك بالأصالة عن نفسه أو كونه الممثل القانوني لأحد الأشخاص الطبيعية أو الاعتبارية، وفي هذه الحالة فإن الإنسان يتخذ جميع خطوات عملية التعاقد الإلكـتروني كطرف، بينما في الجهة الأخرى فإن القرارات تتخـذ مـن جانـب جهـاز الكمبيـوتر المـبرمج مسبقًا، وهذا الشكل من أشكال التعاقد يجب لإتمامه أن يكـون الشـخص الطبيعـي عـلى علم أو من المفترض أن يعلم أن

(1) تعريف الوسيط الإلكتروني وفقا لما ورد في قانون المعاملات والتجـارة الإلكترونيـة الإمـاراتي هـو: برنـامج أو نظام إلكتروني لوسيلة تقنيـة المعلومـات تعمـل تلقائيـا بشـكل مسـتقل، كليًـا أو جزئيًـا، دون إشراف أي شخص طبيعي في الوقت الذي يتم فيه العمل أو الاستجابة له.

الوسيط الإلكتروني المبرمج هو الذي سيتولى العقد معه[1].

2) من كمبيوتر إلى كمبيوتر (باتفاق مسبق) Prior agree: وفي هذه

---

(1) أثيرت إشكالية حول حالة حدوث خلاف بين الإرادة الباطنة و التعبير عنها بمقتضى رسالة البيانات أو أية وسيلة إلكترونية تستخدم في التعاقد،

و لقد أدلي القضاء الفرنسي بدلوه في هذا الأمر، و ذلك في الحكم الصادر من (محكمة ستراسبور)، حيث تتلخص وقائع القضية في أن أحد الأشخاص (Thierry) اشترى (جهاز بروجكتور من نوع سوني) وذلك من على الموقع الخاص بشركة (netbusiness) على شبكة الإنترنت، و كان السعر المعروض علي الموقع هو (خمسة آلاف و مائتان و تسعون فرنكا)، و قد أرسل موقع الشركة له رسالة إلكترونية تفيد تأكيد عقد البيع بمقتضى هذا السعر.

عندما قام (Thierry) بمطالبة الشركة مالكة الموقع بتسليمه جهاز البروجكتور، رفضت الشركة مدعية أن هناك خطأ قد حدث في سعر الجهاز نتيجة لخطأ فني، وأن هذا السعر المعروض على الموقع يقل كثيراً عن السعر الحقيقي.

عندما تم عرض الأمر علي القضاء، استطاعت الشركة أن تثبت أن السعر الذي تم عرض الجهاز به على الموقع لا يساوي 10/1 من السعر الحقيقي له، فاستطاعت الشركة إثبات السعر الذي قامت بشراء الجهاز به و هو (خمسون ألف فرنك) حيث قدمت الفواتير الخاصة بشراء الجهاز، و استطاعت إثبات أن هذا الجهاز يتم بيعه على شبكة الإنترنت على مواقع أخرى منافسة بمبلغ (أربعة و خمسين ألف فرنك)، وإنه يتم بيعه في المحل الخاص بمنتجات شركة سوني بمبلغ (تسعة وخمسين ألف فرنك)، وبالتالي فإن السعر الذي عرض الجهاز به علي شبكة الإنترنت هو سعر غير حقيقي لوجود خلل فني في البرنامج الخاص بالموقع.

أما بالنسبة لرسالة البريد الإلكتروني التي تم إرسالها لتأكيد عقد البيع، فهذه الرسالة يتم إرسالها أوتوماتيكياً بواسطة البرنامج الذي يتولى إدارة الموقع، و بالتالي فهي تتضمن ذات الخطأ الموجود علي الموقع.

حكمت المحكمة في هذه الدعوى ببطلان عقد البيع، و ذلك لانتفاء ركن الرضاء، لأن السعر المعروض علي الموقع الخاص بالشركة لا يعبر عن حقيقة إرادتها.

www.Legalis.net

الحالة فإن العقد الإلكتروني يبرم وينفذ بالكامل بواسطة جهاز كمبيوتر دون تدخل عنصر بشري، ولكن الصفقة التجارية تحدث من خلال مظلة من علاقات تجارية سابقة متفق عليها مسبقًا بين الأطراف المتعاقدة.

3) من كمبيوتر إلى كمبيوتر (بدون اتفاق مسبق) No Prior agree: يتم التعاقد الإلكتروني في هذه الحالة دون تدخل أي عنصر بشري، وبدون وجود اتفاق سابق بين أطراف التعاقد، وفي هذا الشكل من التعاقد يقوم جهاز كمبيوتر بإبرام عقد مع جهاز كمبيوتر آخر ودون أي تدخل من الشخص الذي ينتمي إليه الكمبيوتر.

الفرع الثاني

الحماية المدنية للحقوق الإلكترونية

تعد حقوق الملكية الفكرية وإعادة النشر إلكترونيًا حقوقًا إلكترونية E-Rights وقد تم وضع تصنيف الحقوق التي يشملها موضوع الملكية الفكرية باعتبارها تلك الحقوق التي تتضمن الحق في وضع المصنف الأدبي عبر قاعدة بيانات اتصالية أو في أسطوانة ممغنطة مضغوطة، أو في أسطوانة فيديو رقمية عبر شبكة الإنترنت، أو عبر موقع في شبكة المعلومات الدولية، أو عبر نشرة إلكترونية مثلما هو الحال في أمريكا أون لاين، على سبيل المثال.

وقد وضع الأستاذ الألماني Herbert burkert (أستاذ قانون الاتصالات بجامعة سانت جالن بسويسرا) تصنيفًا للحقوق عبر شبكة الإنترنت ينطلق من حماية التعاملات الإلكترونية لها على أساس التمييز بين الحقوق الشاملة والحقوق الاستثنائية، ومعيار التفرقة هنا أن الحقوق

الاستثنائية مبنية على حرية الاختيار، وذلك على العكس من الحقوق الشاملة، كما أن هذه الحقوق هي حقوق عامة، وأما الأخرى فهي خاصة تخرج عن القاعدة العامة للاتصالات، والتي تتمثل في المشاركة Inclusion ونتعرض لكلا القسمين وفقا للتفصيل التالي[1]:

أولا: الحقوق الشاملة في استخدام شبكة الإنترنت:

وهي أربعة أنواع تنبثق جميعها من اعتبار أن الشبكة تتجاوز الحدود الدولية دون رقابة عليها

1) الحق في الدخول إلى المعلومات the right of access to information لأن إمكانية الحصول على المعلومات المبتغاة هي الغاية من وجود شبكة الإنترنت باعتبارها وسيلة أو أداة تواصلية بين الشبكات دون اعتبار للحدود الدولية، وهذا الحق ذو طبيعة شاملة يتوافق مع فكرة حرية تبادل المعلومات التي قررها المشرع المقارن مثلما هو الشأن في التشريع الفرنسي (القانون رقم 1978/19) الذي ينص في المادة الأولى منه في صدرها على الحرية المعلوماتية وإمكانية إتاحة المعلومات لكل من أرادها.

2) حق التاجر في استخدام شبكة الإنترنت في إنشاء المقر الإلكتروني لتجارته وبث الدعاية حولها، وفتح المجال لتسويق منتجاته للمستهلكين، وذلك باستخدام كافة الأدوات المتاحة على شبكة الإنترنت باعتبارها وسيلة لا تخضع لرقابة الدول، مع الحق في تأمين عمليات

---

(1) أورد الأستاذ الألماني Herbert burker هذا التصنيف في بحثه المقدم إلى مؤتمر روما (8، 9 / 5 / 1998).
at: the Research Center for Information Law at the University of St.Gallen, Switzerland
http//:www.gmd.de/people/herbert.burkert/rom. htm

المبادلة الإلكترونية للسلع والخدمات بشكل عام، وكذلك حق المستهلك المعلوماتي في التسوق عبر الشبكة، بما يستلزمه ذلك من تأمين عمليات المبادلة الإلكترونية التي يقوم بها.

3) الحق الشخصي- الذاتي في الاتصال the right to communication personality والفكرة الأولية في هذا الحق inclusion أنه في بيئة الاتصالات نمارس الحقوق المدنية في اتصالاتنا مع الأقرباء والعائلة والأصدقاء ونتعامل تجاريًا، ويعد البريد الإلكتروني والتوقيع الإلكتروني مثالين على ممارسة هذا الحق، وهذا الحق يعد من الحقوق الشاملة التي لا يجوز مصادرتها أو حذفها، والأثر الشامل للإنترنت على هذا الحق يستلزم ضرورة إقراره وحمايته.

4) الحق في المشاركة الاتصالية: إن حقوق المعلوماتية تقودنا إلى ضرورة المشاركة فيها، ثم إن هذه الحقوق بما تتضمنه من معلومات واتصالات ومشاركة تندمج في مفهوم حقوق المواطنة، فالحق في المشاركة الاتصالية يتطلب بنية أساسية ترتبط بأهمية الاستمرار في المحافظة على الخدمات العالمية للاتصالات بما يفيد التوسع في التجارة الإلكترونية.

ثانيا: الحقوق الاختيارية في استخدام الشبكة الدولية:

تنطلق الفكرة الأساسية فيها من أن الاتصالات ليست من طبيعة عامة وإنما من طبيعة اختيارية، وترتكز نقطة الاختيار هذه على مبدأ حر هو انتفاء فكرة الجبر وهو من مسلمات هذه الحقوق، وتتلخص جملة هذه الحقوق فيما يلي:

1 - الحق في الخصوصية the right of privacy:

ويتضمن هذا الحق مفهوم إمكانية البقاء في عزلة بعيدا عن المشاركة مع الغير، وهو استثناء يجد تطبيقه برفض التعامل مع المؤسسات التي يتطلب الدخول إلى شبكاتها دفع مبالغ مالية، مثل هذه الشبكات إذا لم تتكامل مقومات الدخول إليها فإنها تستمر على خصوصيتها.

2 - الحق في السرية **the right of anonymity**:

تكمن الفكرة الأساسية في هذا الحق في استحالة فرض قيود رقابية على حركة المعلومات واستخدامها في الشبكة العالمية، لذا فإنه وفقًا لهذا الحق يمكن إخفاء المعلومات الشخصية. واستخدام اسم مستعار في إبرام العقود الخاصة بالتجارة الإلكترونية بشرط ألا يكون ذلك من شأنه إخفاء أساليب احتيالية.

3 - الحق في عدم الظهور **the right of non-availability**:

إن هذا الحق يعد أحد أهم آثار عدم خضوع الشبكة الدولية الإنترنت للرقابة من الدول، فيمكن عدم الظهور دون أن يكون لذلك عقاب ما، وإن أكثر بروز لهذا الحق حال التعامل الإلكتروني من خلال مواقع ليس لها وجود في الواقع المادي، وإنما لها وجود في الواقع إلكتروني، وهذه مسألة أثارت جدلا في الفقه حول مدى المشروعية خصوصًا إذا كان لهذا الفعل آثار ضارة على بيئة التجارة الإلكترونية.

4 - حق المستخدم في قوة موقفه

the right of user empowerment:

يعني هذا الحق أن للمستخدم كامل الحرية في الدخول أو عدم الدخول إلى المواقع الإلكترونية، وحقه في إخراج ذاته عن مضمون المعلومات

المتوافرة، وإيجاد الوسائل الدفاعية المناسبة له للحيلولة دون تصاعد المخاطر دون أن تكون الوسيلة الوحيدة في ذلك هي إغلاق الجهاز أو فصل جهازه عن الشبكة، ويلزم لاستخدام هذا الحق التدريب على إيجاد خيارات آلية دفاعية، تساعد على حماية الذات ضد العدوان باستخدام الشبكة المعلوماتية، أو على ما تحتويه هذه الشبكة كالبيانات والمواقع والبريد الإلكتروني والتجارة الإلكترونية[1].

الفرع الثالث

المسئوليات والالتزامات المدنية

هناك العديد من الالتزامات والمسئوليات في نطاق العالم الافتراضي، والمتصلة بشكل مباشر بالتجارة الإلكترونية، والتي من الواجب توفير أقصى درجات الحماية لها، وهي كما استخلصناها من تصنيف الأستاذ burker السابق بيانه[2] وتطبيقه على موضوع التجارة الإلكترونية، ونستطيع إيجاز الكلام في هذا الصدد فيما يلي:

1 - الالتزامات تقابل الحقوق

يرتب الإخلال بالالتزام الذي يفرضه القانون المسئولية القانونية، وذلك من منطلق أن الالتزام أو المسئوليات إنما هي مرآة الحقوق، وفي مجال التجارة الإلكترونية فإن الحق في حرية التعاقد، والحق في حرية إنشاء مقار التجارة الإلكترونية، وحق المستهلك في الدخول إلى تلك المقار لإبرام عقود شراء السلع والخدمات يقابلها مسئولية صاحب المقر في حالة الإعلان الوهمي عن السلع والخدمات، وكذلك مسئوليته عن الغش التجاري.

---

(1) http// www.msh.paris.fr/red&s/index.htm

(2) http//www.gmd.de/people/herbert.burkert/rom. htm

كما يقابل الحقوق الخاصة بالتاجر والمستهلك مسئولية الغير إذا تعمد الدخول غير المشروع إلى هذه المواقع، واستعمال المعلومات الخاصة بها أو إتلافها أو سرقتها أو سرقة الأموال التي تتم عبر الوسائط الإلكترونية عن طريق مبادلة السلع والخدمات، وكل ذلك يلقي على الدولة التزامًا بالحماية من خلال توثيق المعلومات عبر موثق الخدمة، ويعد ذلك أكبر تحدٍّ يواجه الدولة لأن الإخلال به يعد من أكبر معوقات التجارة الإلكترونية.

2 - التزامات ومسئوليات جديدة:

خلق التقدم في التقنيات الخاصة بالكمبيوتر وملحقاته وارتباط التجارة الإلكترونية به التزامًا بضرورة حماية السوق الإلكتروني العالمي، والذي يعتمد بصورة رئيسة على المستهلك الإلكتروني؛ لذا فإن الفقه والقضاء استقرا على وجود الالتزام بالتعاون بين أطراف التجارة الإلكترونية، ويشمل هذا الالتزام عدة التزامات تتفرع عنه وهي كالآتي:

- الالتزام بمنتهى حسن النية في التفاوض الإلكتروني، بمعنى أن تتسم عملية التفاوض بالنزاهة والأمانة والثقة، مع الامتناع عن كل ما من شأنه إعاقة المفاوضة، أو محاولة التضليل للإضرار بالطرف الآخر.
- الالتزام بالإعلام، أي أن يعلم كل طرف الآخر بما لديه من معلومات تتعلق بالبيانات والمعلومات الخاصة بالتجارة الإلكترونية والعقد مما قد يكون له أهمية في إبرام التعاقد حتى تتسم العملية بكاملها بالشفافية.
- الالتزام بتقديم النصح والإرشاد بشأن موضوع العقد، ويأتي هذا الالتزام نتيجة لتفاوت الخبرات الخاصة بالعقود، خصوصًا تلك التي تتسم بالتقنية العالية والتي قد تفرض التزامًا على المورد نفسه بتقديم النصيحة للمتعامل معه نظرًا لاحترافه هذا المجال، وهذا الالتزام هو التزام مكمل للالتزام الخاص بالإعلام، وينطبق بالدرجة الأولى على

التعامل في الأشياء التي تنطوي على مخاطر تهدد أمن العميل وسلامته.

- الالتـزام بالمحافظـة عـلى الأسرار، بموجـب هـذا الالتـزام يلتـزم كـل مـن المـورد والعميـل بالمحافظة على الأسرار، وهو التزام تبادلي يتسع نطاقـه ليشـمل الأسرار الخاصـة بالعمليـة التفاوضية التي قد تتطلب أحيانًا أن يكشف أحد الأطراف للطرف الآخر عن بعض أسراره الفنية والمهنية [1].

الفرع الرابع

بعض الحقوق التي صادفت مشكلات في الحماية المدنية

أثارت بعض الحقوق المدنية في العالم الافتراضي العديد من المشكلات

---

(1) انظر طعن دستوري مصري رقم 106 لسنة 19 ق، جلسة 2000/1/1 (المحامي، مصر- ع.1 لسنة 2001، ص291) حيث جاء في هذا الطعن: " إنه من المقرر أن السلطة التي يمتلكها المشر-ع في مجال تنظيم الحقوق حدها قواعد الدستور التي تبين تخوم الدائرة التي لا يجوز اقتحامها، وبما ينال من الحق محل الحماية أو يؤثر في محتواه، ذلك إن لكل حق دائرة يعدل فيها ولا يتنفس إلا من خلالها، فلا يجوز تنظيمه إلا فيما وراء حدودها الخارجية، فإذا اقتحمها المشر-ع كان ذلك أدعى إلى مصادرة الحق أو تقييده". كما قضت المحكمة ذاتها في الطعن الدستوري رقم 163 لسنة 200ق. جلسة 2000/8/5 (السابق ص 367) بأنه: " وحيث إن الأصل في سلطة المشر-ع في موضوع تنظيم الحقوق أنها سلطة تقديرية ما لم يقيد الدستور ممارستها بضوابط تحد من انطلاقها وتعتبر تخومًا لها لا يجوز اقتحامها أو تخطيها، وكان الدستور إذ يعهد إلى أي من السلطتين التشريعية والتنفيذية بتنظيم موضوع معين، فإن القواعد القانونية التي تصدر عن أيتهما في هذا النطاق لا يجوز أن تنال من الحقوق التي كفل الدستور أصلها سواء بنقضها أو انتقاصها عن أطرافها، وإلا كان ذلك عدوانا على مجالاتها الحيوية من خلال إهدارها أو تهميشها.

وخاصة في مجال الحماية المدنية لهذه الحقوق، ومن هذه الحقوق ما يلي:

1 - الحق في الخصوصية والمحافظة على الأسرار:

فإذا تأملنا الإطار العام للحماية المدنية فإن الحق في الخصوصية يقف على قمة الهرم، إذ وقـف التشريع في غالبية الدول لكل محاولة للعدوان على هذا الحق عبر شبكة الإنترنت، ففـي الولايـات المتحـدة الأمريكيـة وقـف قانون خصوصية الاتصالات الإلكترونية بالمرصـاد لإدارة البحريـة الأمريكيـة[1]، ومثـال ذلـك قضـية Timothy R. McVeigh، v. William Cohen[2]، حيث قضت المحكمة الابتدائية لولاية كولومبيا بإلغاء كافة

---

(1) Eric. j. sinrod،barak D.jolish. controlling chaos: the emergion law of privacy and speech in cyberpace. Op،cit p.5.

(2) Timothy R. McVeigh, v. William Cohen, January 26, 1998

Plaintiff, a Navy serviceman, sent an anonymous e،mail via AOL under the alias "boysrch." The recipient searched through AOL's member profile directory, which indicated that "boysrch" was a homosexual. The member profile did not identify "boysrch" as plaintiff. The receipent forwarded this information to the Navy. In response to a subsequent inquiry from the Navy, AOL identified "boysrch" as plaintiff. Defendant thereafter held an administrative hearing at which it determined that plaintiff should be discharged for engaging in homosexual conduct.

On plaintiff's motion, the Court issued a preliminary injunction enjoining the Navy from discharging plaintiff.

"Suggestions of sexual orientation in a private anonymous e،mail account [do] not give the Navy a sufficient reason to investigate to determine whether to commence... discharge proceedings. In its action, the Navy violated" its Don't Ask, Don't Tell, Don't Pursue policy.

The Court further found that the Navy's request that AOL identify the true identity of "boysrch" was "likely illegal" under the Electronic Communications Privacy Act of 1996, 18 U.S.C. §2703. "The ECPA... allows the government to obtain information from an online service provider... only if a) it obtains

الإجراءات التي تمت بالمخالفة لهذا القانون؛ لأن الإجراءات تلك قد تمت بدون الحصول على الإذن من السلطات القضائية المختصة وفقًا لقانون الإجراءات الجنائية، في حين أن البعض الآخر من الدول لم يجعل لهذا الحق الأولوية في القانون.

2 - حقوق الملكية الفكرية:

ظلت حقوق الملكية الفكرية تشغل المشرع على المستويين الدولي والمحلي، وإن كان الوضع الدولي قد أخذ أسبقيته على التشريعات الوطنية، نظرًا لأن العديد من الاتفاقيات الدولية قامت بتناول هذا الموضوع وتنظيمه، مما أحاطه بأهمية ارتقت إلى مستوى الحقوق الدستورية[1]، فالمادة 8/1 من الدستور الأمريكي قد نظمت هذا الحق[2].

ولقد ترتب على دخول حقوق الملكية الفكرية في دائرة الحقوق الإلكترونية أن اتسعت دائرة حقوق التأليف والنشر لتشمل حقوقًا جديدة، مثلما هو الحال في شرط منح الحقوق، وشرط مستقبل التكنولوجيا، وبمقتضاها يمنح المؤلف الناشر الحق في التداول الإلكتروني لمؤلفه.

---

a warrant issued under the Federal Rules of Criminal Procedure or state equivalent; or b) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question." Having failed to follow either path, the Navy ran afoul of the ECPA. The court rejected the government's argument that §2703(c) only prohibits the actions of Internet Service Providers, and not the Government.

(1) Losey R.C، practical 7 legal protection of computer database p. 2. Available online in march 2000 at:
http://www.uplink.com.au/lawlibrary/document/docs/doc32.htm

(2) " To promote the progress of science and useful arts، by securing for limited ties to authors & inventors the exclusive right in their respective writings & discoveries".

ففي قضية tasinin v. Newyourktimes co. التي عرضت على المحكمة الفيدرالية بشأن جواز النشر بالتداول الإلكتروني لأعمال الصحفيين المستقلين بوضعها على شبكة الإنترنت.

والمبدأ الذي قررته المحكمة هو حق النشر والعرض الإلكتروني، والذي يصح أن يكون محلا لتملك الناشر الإلكتروني[1]، وهذا الحق يعد من قبيل الحقوق المطلقة للناشرين دون حاجة إلى موافقة مسبقة من قبل المؤلف، إذ إن حق العرض التكنولوجي ليس منفصلا عن العرض العادي، وذلك وفقًا لما هو مقرر في قانون النشر الأمريكي[2].

وفي النهاية فإن هناك ضرورة للمراجعة الشاملة والجادة من قبل الأنظمة الوطنية في جميع أنحاء العالم للنظام الدولي للنسخ وحقوق المؤلف، حتى يمكن تأمين أعمال الفنانين والكتاب والناشرين والموسوعيين، وشركات التسجيل ومبرمجي الحاسوب وشبكة الإنترنت من انتهاك أعمالهم في كل مكان، وليس في بلدانهم فقط[3]، ويشمل هذا الموقف الاتفاقيات الجديدة التي دخلت حيز النفاذ مع بداية العام 2001 في العديد من بلدان العالم كبرنامج دولي لحماية حقوق الملكية الفكرية.

---

(1) the ownership of a copyright may be transferred in whole or in part by any means of conveyance or by operation of law"

(2) "any of exclusive right. Compromised in a copyright، including any subdivision of any rights may be transferred... and owned separately".

(3) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 138.

المطلب الثالث

الحماية الاقتصادية للتجارة الإلكترونية

تزايد حجم التجارة الإلكترونية حتى أضحت تمثل شريان الاقتصاد في الوقت الحاضر وفي المستقبل، حيث تؤكد الإحصائيات أن أكثر من ربع مستخدمي شبكة الإنترنت هم من المتعاملين في حركة التجارة الإلكترونية، ويستفيدون من خدماتها ما بين موردين وعملاء.

ونظرًا للجانب الاقتصادي المهم في التجارة الإلكترونية فقد وجدنا أن هناك نوعًا من الحماية وفرها الجانب الاقتصادي التجاري المتصل بالتقنية، من خلال النظم واللوائح والقرارات المنظمة لعملها من جهة، والإجراءات والوسائل التجارية من جهة أخرى.

وقد قامت العديد من الشركات البرمجية بتطوير برامج لحماية المعلومات وصحتها وأمنها سواء المتبادلة منها أم تلك المخزنة على الدعامات، ويتوخى من برامج الحماية تأمين الوثوقية والسرية في نقل المعلومات، والتحقق من هوية الأشخاص الذين يستخدمون مواقع التجارة الإلكترونية، ومن أجل إجراء عمليات الدفع على الشبكات الاتصالية إلكترونيًا قامت بعض الشركات - بالتعاون مع المصارف - بتطوير آليات للدفع الإلكتروني وفقا لما يتناسب مع الأوضاع الاقتصادية والتجارية والتقنية المتناسبة مع التجارة الإلكترونية.[1]

(1) ومن هذه الوسائل المستخدمة في الدفع الإلكتروني بطاقات الائتمان Credit Cards والبطاقات الذكية Smart Cards والنقود الرقمية Digital Money والنقد الإلكتروني E-Cash وطرق أخرى، وتطور حاليًا بعض البروتوكولات الأساسية للنقد الإلكتروني والتي تتميز بوثوقية وحماية في نقل المعلومات، ومن هذه البروتوكولات: طبقة القبس الأمين Secure Socket Layer (SSL) والمداولة=

ويمكن القول بأنه من خلال الفكر الاقتصادي والتجاري عبر شبكة الإنترنت أمكن التوصل إلى الكثير من الفوائد رغم ما يثار من مشكلات في إطارها، والتي تأخذ الطابع التقليدي في ظاهرها، وتستند إلى مفاهيم تقليدية في فهمها، وسوف نتناول المدلول الاقتصادي للتجارة الإلكترونية، ومفهوم الحماية الاقتصادية في فرعين مختلفين فيما يلي:

الفرع الأول

المدلول الاقتصادي للتجارة الإلكترونية

لقد لاحظ Bill Gates المفارقة بين فكرة الاقتصاد التقليدي وبين فكرة الاقتصاد الرقمي عبر شبكة الإنترنت مؤكدًا على أن الانتصار حليف الأخير مستقبلا[1]، ويشير الفقه إلى أن للتجارة الإلكترونية جذورًا تمتد إلى القرن

= الإلكترونية الأمنية Secure Electronic Transaction (SET), ومن أجل تحسين تسويق المنتجات والسلع والخدمات على شبكة الإنترنت يجري تطوير برامج لإدارة العلاقة مع الزبون Customer Relationship Management (CRM) مما يساعد على إعداد تطبيقات ومواقع تلبي حاجة الزبون ورغباته، وكذلك تستخدم الشركات تطبيقات لإدارة سلسلة الإنتاج Supply Chain Management (SCM) ضمن الشركة الواحدة أو بين عدة شركات، مما يساعد على تقليص زمن تسليم البضائع بنسبة تتراوح بين 20٪ و40٪، ويقلل من ضرورة توفر المخزون بنسبة تتراوح بين 15٪ و25٪، ويخفف من تكلفة العمل الإداري بنسبة تتراوح بين 30٪ و70٪.

www.arab ency.com / index.php?module=pnEncyclopedia&func =display_term&id=159758

(1) stataments by Bill Gates. Redmond wash may 24 2000. Press pass،microsoft page. Available onolin in june 2000 at:
http://www.microsoft.com/presspass/features/2000/ceosummit/os،24gates.asp

التاسع عشر، فقد وجد في أحكام القضاء المقارن القديمة حكم اعتمد القضاء الأمريكي فيه التلغراف كأساس للتعاقد، كان ذلك في عام 1869 حينما قررت محكمة New Hampshire الأمريكية في قضية Howley v. Whipple. 48 N.H 487(1869) أن تبادل الإرادة عبر التلغراف أمر كاف لقيام عقد في هذا الشأن، ثم تطور الأمر لكي يعتمد القضاء أيضًا ولكن في زمن متأخر أدوات الاتصال التي استحدثت بعد ذلك كالتلكس والفاكس، بحيث أصبح عاديًا أن يتم تبادل الإرادة من قبول وإيجاب بهذا الأسلوب.

وسبق أن بينا أن التجارة الإلكترونية في المفهوم الاقتصادي هي تلك التجارة التي تقتصر على تداول السلع دون عمليات الإنتاج والتصنيع، ويتم ذلك عبر وسائل الاتصال الحديثة ومن أهمها شبكة الإنترنت العالمية، وذلك بقصد جعل المعاملات التجارية تجري بصورة تلقائية وسريعة.

ويرجع المفهوم الرقمي للتجارة الإلكترونية حقيقة إلى ثمانينيات القرن الماضي، حيث كان التوجه أكثر تخصيصًا في النظام الأمريكي فيما يعرف بمصطلح التبادل الإلكتروني للبيانات، الذي يمكن تعريفه بأنه "تبادل معلومات الأعمال من حاسوب إلى آخر بنظام هيكلة البيانات".

ثم استخدمت الأمم المتحدة مصطلحًا أكثر تعميمًا هو تبادل المعطيات المعلوماتية في مجال الإدارة والتجارة والنقل[1].

وحتى الآن لم يتمكن فقه القانون والاقتصاد والسياسة من إرساء قواعد بنيان قانوني متكامل لموضوع التجارة الإلكترونية على الرغم من الاتفاق العام على موضوعها، ويمكن القول إجمالا بأن التعامل بنظم الوفاء

(1) د. محمد السيد عرفة، التجارة الدولية الإلكترونية عبر شبكة الإنترنت ومفهومها، والقاعدة القانونية التي تحكمها، ومدى حجية المخرجات في الإثبات، مرجع سابق، ص 6.

بالتحويل الإلكتروني لا يزال في مقدمة النشاط المالي والتجاري والاقتصادي الذي يحظى باهتمام تشريعي، فهو كوفاء بالتزام بالوسائل الإلكترونية[1] يجعل نظم الوفاء بالتحويل الإلكتروني محلا للجدل في الفقه والقانون سيما الجنائي منه، خاصة فيما يتعلق ببطاقات الائتمان التي تتعرض لعدوان عبر شبكة الإنترنت[2].

ويستمد الأساس الذي تبنى عليه فكرة التجارة الإلكترونية من معايير التجارة الحرة التي ترى أن قوة التجارة تنبع من ذاتها، ولا تحتاج إلى تقييد بقصد المحافظة على المصالح التجارية، فيبطل كل تشريع يقيد حرية التجارة الإلكترونية، التي خلقت عالمًا تجاريًا إلكترونيًا لم يكن له وجود قبلها، وهذا هو عالم المنتجات الإلكترونية التي جعلت من المعلومة سلعة بعد أن كانت مجرد خدمة عادية بغير قيمة اقتصادية في عالم المستهلك.

ولعل من المظاهر التجارية الجديدة عبر التجارة الإلكترونية - كما أسلفنا - المركز التجاري الافتراضي، وهو عبارة عن خدمة إلكترونية يتم الدخول إليها عبر شبكة الإنترنت بالنظام المفتوح، تسمح بالعرض والطلب من خلالها[3].

فهذا المركز يتشابه مع المراكز التجارية في العالم المادي، إلا أنه

(1) ويتم بتوجيه أمر من قبل المدين إلى مصرفه لوفاء التزام بذمته بوسيلة إلكترونية إلى دائنه، أو بتوجيه أمر من المدين إلى مصرفه بتحصيل مبلغ من حساب دائنه، بناءً على تفويض مسبق بوساطة إلكترونية، راجع د. فياض ملفي القضاة، مسئولية البنوك الناتجة عن استخدام الكمبيوتر كوسيلة وفاء، مؤتمر القانون والكمبيوتر والإنترنت،جامعة الامارات، المجلد الأول، ص 16.

(2) د. جميل عبد الباقي الصغير - الحماية الجنائية والمدنية لبطاقات الائتمان - المرجع السابق، ص 35.

(3) http://www.grolier.fr/evberlexnet/com/a980902.htm

يختلف عنها في كون المتجر المادي له موقع معين تتجمع فيه المحال التجارية ككل، في حين أن المركز الافتراضي تتجمع فيه المحال التجارية في موقع افتراضي، وقد تكون هذه المحال مختلفة في أماكن وجودها المادي، كما لو كان أحد المحال في روما، والثاني في دبي، والثالث في القاهرة، والرابع في نيويورك.

ولقد أخذ الوضع الدولي مجراه في الاهتمام بتجارة الخدمات، والتي من أهم أركانها خدمة المعلومات التي أشارت إليها جولة أورجواي، والتي تم فيها إدماج الخدمات في نظام الجات (الاتفاقية العامة للتجارة في الخدمات في 1993/12/15)[1] فإذا أضفنا إلى ذلك ما تحققه التجارة الإلكترونية من إيجابيات في إطار التعاملات المالية عبر العالم، حتى إن اتجاهًا جديدًا لدى الاقتصاديين يرى عدم إمكانية استمرار الائتمان في مواجهة متطلبات هذه التجارة لضخامة حجمها، ويتجه إلى إبراز فكرة أموال خاصة بشبكة الإنترنت والتجارة الإلكترونية.

ولقد تنبهت دول كثيرة ذات مصلحة في التجارة الإلكترونية لخطورتها وحجمها ومدى أهميتها من حيث ما تحدثه في الاقتصاد العالمي، وعلى رأس هذه الدول الولايات المتحدة الأمريكية التي عبرت عن فهم عميق لمدى أهمية التجارة الإلكترونية على لسان نائب الرئيس الأمريكي الأسبق آل جور الذي نشر مقالا في مجلة جامعة هارفارد للقانون والتكنولوجيا، تحدث فيه عن فكرة البنية التحتية للمعلومات، باعتبارها البنية التي ينبغي أن تسود قائلا: "نحن نتحدث عن البنية التحتية للمعلومات كما لو كانت شيئًا ما،

(1) د. صفوت عبد السلام عوض الله، تحرير تجارة الخدمات في ظل اتفاقية الجات وانعكاساتها على اقتصاديات الدول النامية، مجلة العلوم القانونية والاقتصادية، العدد الأول، سنة 40، يناير 1998، ص 64.

منتجًا ما، مجموعة قطع صلبة وبرمجيات ستلايت وهواتف، ومقسمات وألياف بصرية، إنها ذلك كله بالإضافة إلى المزيد أيضًا، إنها معنى يقوم بتغيير رؤيتنا للجهد الإنساني.[1]

وأعقب ذلك إصدار الولايات المتحدة الأمريكية نموذج عمل التجارة الإلكترونية في أول يوليو 1997، موقعًا من الرئيس الأمريكي بيل كلينتون ونائبه آل جور، ويتضمن النموذج المذكور ما ينبغي على الدول تجنبه حين التعامل بالتجارة الإلكترونية، فهو محاولة لفرض مفاهيم السوق حين تتناول تلك الدول موضوع التجارة الإلكترونية عبر شبكة الإنترنت بالتنظيم.

الفرع الثاني

مفهوم الحماية الاقتصادية

الحقيقة أن مجرد قيام هذه الدولة أو تلك أو حتى المجتمع الدولي باتخاذ خطوات تشريعية تجاه تنظيم ظاهرة التجارة الإلكترونية إنما هو ضرب من محاولات متواصلة لفرض حماية لها، على أن الفرض هنا يقتضي بالطبع أن تكون هذه الحماية التنظيمية من ذات الطبيعة التي عليها فكرة التجارة الإلكترونية، حيث إنها من طبيعة حرة بأقصى ما يمكن أن يصله مفهوم الحرية من مدلول، وهذا أمر تجب مراعاته حسمًا للعديد من المشكلات التي من الممكن أن تقوم خاصة في إطار التجريم والعقاب والمسئولية الجنائية، والحل الأمثل يظل هنا هو السعي وراء حلول معضلات التجارة الإلكترونية في شكل عالمي بداية، باعتبار أنها تمس قضايا عالمية، فعملية نقل المنتج المطلوب في الحالات التي يتم فيها ابتياع منتج مادي مثلا قد تشكل عقبة تبدأ من تكاليف النقل خصوصًا إلى الجهات التي تكون فيها وسائل النقل

(1) At: www.iitf.nist.gov/eleccomm/ecomm.htm

منعدمة أو غير متفقة مع التطورات الحديثة، في حين أن تكاليف النقل في الدول التي ترفع شعار التقدم هي أسهل بكثير[1].

وعلى ذلك فإن نقاط الاتفاق والاختلاف في المدلول الدولي يكون مرتكزًا على حماية المستهلك بالدرجة الأولى، حتى إن مجلس الدولة الفرنسي في تقريره حول شبكة الإنترنت في عام 1998 قرر لزوم إبرام اتفاقية دولية تتضمن معايير لحماية المستهلك عبر شبكة الإنترنت، فالمستهلك النهائي يمثل - كما هو الشأن في أنواع التجارة الأخرى - القاعدة التي ترتكز عليها التجارة الإلكترونية لكونه الهدف النهائي في العملية التجارية، ولقد كان تقنين ما يعرف الآن بالتعاقد عن بعد نموذجًا حيًّا لموضوع حماية المستهلك عبر شبكة الإنترنت، وهي نوعية من العقود تستهدف تنوع الاتصالات، وأهمها تلك الناجمة عن التجارة الإلكترونية عبر شبكة الإنترنت التي تختلف تمامًا عن فكرة البيع عن طريق التليفزيون، والهدف من تقنين هذه العقود هو حماية المستهلك الإلكتروني[2].

وإذا تأملنا موضوع حركة المعاملات المالية عبر شبكة الإنترنت في إطار التجارة الإلكترونية فإن المشكلة تظل في إطار حماية سرية هذه المعاملات المصرفية، وما يتعلق بسرية بياناتها، وعدم كشفها من قبل الغير.

إن هذه القضايا جعلت موضوع التجارة الإلكترونية ذا أهمية كبيرة لدى

---

(1) William E.wyrough. Jr. *AND Ron Klein، the electronic signature act of 1996: breaking down barriers to widespread electronic commerce I Florida p. 410، Florida state university law review (vol.24: 407).

(2) د. محمد السيد عرفة، التجارة الدولية الإلكترونية عبر شبكة الإنترنت ومفهومها والقاعدة القانونية التي تحكمها، ومدى حجية المخرجات في الإثبات، مرجع سابق، ص7.

الفقه والتشريع، خصوصًا ما يتعلق بتجريم العدوان على وسائل وأدوات التجارة الإلكترونية[1]، وتحركت كثير من الدول لسن التشريعات لتنظيم التجارة الإلكترونية.

فقد أرسى التوجيه الأوروبي بشأن التجارة الإلكترونية الصادر في 2000/6/8 اهتمام المشرع الأوروبي بفكرة المجتمع المعلوماتي كمصطلح تبنى عليه فكرة التجارة الإلكترونية.

وتم إعداد مشروعات قوانين تتعلق بالنظام القانوني لتكنولوجيا المعلومات في المجتمع الكندي قدمت إلى الجمعية الوطنية تضمنت تحديدًا لتكنولوجيا المعلومات، وتعريفًا قانونيًا لها دخل إلى حيز التنفيذ في 2000/11/16، ويعترف هذا القانون بالعقود الإلكترونية، وكذلك بالتوقيع الإلكتروني، وجعلهما في مستوى نظيريهما في العالم المادي.

أما نموذج عمل التجارة الأمريكية لسنة 1997 فقد تضمن خمسة مبادئ تسترشد بها الحكومة - وأية حكومة - في تنمية وتطوير فكرة التجارة الإلكترونية، وهذه المبادئ هي:[2]

1) وجوب تولي القطاع الخاص الدور القيادي، بحيث يتم تطوير شبكة الإنترنت على ضوء اقتصاديات السوق دون الخضوع لقيود تنظيمية.

2) وجوب تقليص الدور الحكومي بحيث تتجنب الحكومات التدخل غير الضروري في الاتفاقيات التجارية عبر شبكة الإنترنت.

3) وجوب تأمين المنافسة، وحماية الملكية الفكرية، وحظر الغش وتقوية

(1) world online. Robert bond، the privacy war، oct.2000. available online in oct. 2000 at: http://2163.11671/ipw/articles/ipwa01.htm

(2) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 148.

الشفافية، والمساعدة في حل المنازعات.

4) إدراك الحكومات لخصائص شبكة الإنترنت المتميزة من حيث كونها ذات طبيعة غير مركزية، وعابرة للحدود الدولية، وتقوم على التقنية المعلوماتية.

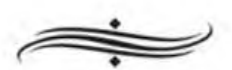
5) يلزم العمل على تسهيل شبكة الإنترنت في المجال العالمي باعتبارها سوقًا عالمية.

وخلاصة القول أن النظم الإقتصادية القائمة من قوانين ولوائح تستطيع توفير الكثير من الحماية لهذه التجارة من خلال وضع آليات حماية قوية لجميع المتعاملين تضمن الخصوصية، وحماية المعلومات، والسرية وتنظيم استخدام التوقيع الالكتروني، ووسائل التشفير المتعددة، وشهادات التعريف الرقمية والالكترونية, ووسائل الدفع الالكتروني, والعمل على تعزيز الثقة في التجارة الالكترونية بين الشركات والمؤسسات التجارية من جهة والأفراد من جهة أخرى, وفي وسائل هذه التجارة وأدواتها.

كما أنه يجب أن تضطلع النظم الإقتصادية أيضا بضرورة تثقيف الأفراد والمؤسسات بالطرق المثلى لاستخدام التجارة الالكترونية, لاختلافها بصورة كبيرة عن التجارة التقليدية, وكذلك بيان الأساليب المثلى لحماية الشركات والأفراد من الاختراقات التي تتعرض لها هذه التجارة بصفة مستمرة, والاعتداء عليها.

وأخيراً علينا أن ندرك مدى أهمية التجارة الإلكترونية لدعم وتنمية الاقتصاد الوطني، وتعزيز التجارة المحلية والخارجية والتبادل التجاري، وزيادة القدرة التنافسية لصادرات السلع والمنتجات الصناعية من خلال تسويقها إلكترونيا. وأن الأمر يستحق العناية والدعم من قبل الأنظمة الاقتصادية ذات العلاقة، حيث إن ازدهار التجارة الإلكترونية يتوقف على

وجود اقتصاد متطور ذي قاعدة إنتاجية متسعة ومرنة، وكذلك شبكة اتصالات وبنية معلوماتية كاملة، وهذا من أجل تكوين اقتصاد رقمي يعتمد على الإنتاج الكثيف للمعلومات والتقنية المتطورة.[1]



(1) http://www.aleqt.com/2009/01/15/article_184514.html

الفصل الثالث

تجارب التنظيم القانوني للتجارة الإلكترونية

تمهيد وتقسيم:

أدركت منظمات الأعمال والتكتلات الاقتصادية أهمية تبادل البيانات التجارية إلكترونيًا في إنجاز أعمال التجارة الإلكترونية، وضرورة وجود تنظيم قانوني متعلق بجوانب التجارة الإلكترونية، وما يرتبط به من فائدة لضبط نظم التبادل الإلكتروني للبيانات التجارية، والتنسيق بين التنظيمات القانونية للتجارة الإلكترونية، وشكل التبادل الإلكتروني للبيانات بين أطراف التعامل في الدول المختلفة[1].

وتعددت الجهود الدولية الرامية إلى تنظيم طرق التجارة الإلكترونية بقواعد اتفاقية، إلا أن أهم هذه الجهود كانت من لجنة القانون التجاري الدولي التابعة للأمم المتحدة[2]، والتي أعدت قانونا نموذجيًا للتجارة الإلكترونية استهدفت به تقديم مجموعة من القواعد المقبولة دوليًا، والتي يمكن أن تساعد الدول عند سن تشريعات لتجاوز العقبات القانونية التي تعوق استعمال وسائل الاتصال الإلكترونية في التجارة الدولية، وإلى جانب ذلك فقد تضمن هذا القانون النموذجي مجموعة من المبادئ، الهدف منها تقديم إرشادات لمستخدمي وسائل الاتصال الإلكترونية، في سبيل إيجاد حلول للصعوبات القانونية التي تعترض التجارة الإلكترونية،

(1) ويقصد بذلك تكوين الرسالة الإلكترونية، وأنماط تبادل البيانات، وإشعار استلامها، وتسجيل وتخزين البيانات ووسائل حمايتها.

(2) يطلق على لجنة الأمم المتحدة للقانون التجاري الدولي اختصارًا مصطلح اليونسترال Unictral.

وبالإضافة إلى إصدار القانون النموذجي للتجارة الإلكترونية، فإن لجنة الأمم المتحدة للقانون التجاري الدولي وضعت مجموعة قواعد موحدة للتوقيع الإلكتروني كأداة من أدوات توثيق عقود التجارة الإلكترونية.

وإذا كانت أعمال لجنة الأمم المتحدة لقانون التجارة الدولية (الأونسيترال) فيما تصدره من قواعد نموذجية أو موحدة لمتطلبات التجارة الإلكترونية تؤدي إلى التوحيد والتنسيق بين القوانين الوطنية، فإن منظمات الأعمال والتكتلات الاقتصادية الأخرى تؤكد على أن التنظيم القانوني للظواهر الاقتصادية الذي ينفرد أصحاب المصلحة بوضعه في شكل قواعد للسلوك، ويكتسب قوته الإلزامية من جريان العمل به، يعد الوسيلة الطبيعية لضبط التعامل الداخلي لأرباب الصناعة أو التجارة فيما بينهم وبين من يتعاملون معهم، باعتباره تنظيما ذاتيًا للظاهرة الاقتصادية، في حدود ما تقتضيه مصالحهم، إلا أن تداخل المصالح الفردية مع المصالح العليا للدولة في بعض الحالات، يؤدي إلى وضع قواعد عامة لتنظيم السلوك الواجب اتباعه فيما يجاوز الحدود المسموح بتنظيمها ذاتيًا، وبالتالي إذا تجاوزت الظاهرة تلك الحدود فإنها تدخل في إطار التنظيم الذي وضعته الدولة لها، وهو ما ينطبق على نموذج التجارة الإلكترونية.

ونظرًا لأن استخدام الوسائل الإلكترونية في إنجاز الأعمال التجارية قد يمس مصالح عليا للدولة فإن ذلك يقتضي تنظيمه بقواعد تتعلق بالنظام العام، كتلك المتعلقة بحماية المستهلك، وحماية حقوق الدولة، كحقها في استيفاء الرسوم والضرائب وملاحقة أشكال الإجرام الجديدة على شبكات الاتصال، لهذا فمن الضروري أن تتولى الدولة وضع القواعد المتعلقة بقطاع التجارة الإلكترونية، ويقتضي ذلك النظر في إرشادات أو

تجارب التنظيم القانوني للقواعد المراد تنظيمها، وهو الأمر الذي تقتضيه مصلحة الدولة المشرعة.

كما كان لمجتمع المعلومات دور كبير في تنظيم التجارة الإلكترونية من خلال قمة المعلوماتية، والتي تمثل عملية تعددية حقيقية لأصحاب المصلحة الذين يشملون الحكومات والمنظمات الدولية الحكومية والمنظمات غير الحكومية والقطاع الخاص والمجتمع المدني، وهدف القمة هو بناء مجتمع معلومات جامع يتجه نحو التنمية، مجتمع يستطيع كل فرد فيه استحداث المعلومات والمعارف والنفاذ إليها واستخدامها وتقاسمها، ويتمكن فيه الأفراد والمجتمعات والشعوب من تسخير كامل إمكانياتهم للنهوض بتنميتهم المستدامة لتحسين حياتهم، فكانت قمة المعلوماتية الأولى والثانية.

وسوف نعرض لذلك وفق المباحث التالية:

المبحث الأول: التجارة الإلكترونية في المنظمات الدولية والإقليمية

المبحث الثاني: التجارة الإلكترونية ومجتمع المعلومات

المبحث الثالث: التجارة الإلكترونية في التشريعات الوطنية



المبحث الأول

التجارة الإلكترونية في المنظمات الدولية والإقليمية

توجهت أعمال العديد من المؤسسات الدولية المعنية بشئون التجارة إلى إزالة العقبات القانونية التي تعترض استخدام نظم التعامل الإلكتروني في التجارة، وسعت إلى توفير البيئة المناسبة لنشر التجارة الإلكترونية بإصدار السياسات والتشريعات اللازمة، وتعزيز الآليات الإقليمية لزيادة التبادل التجاري إلكترونيًا بين الدول المختلفة، وإزالة العوائق التي تعوق تدفق التعاملات التجارية.

فقامت لجنة القانون التجاري الدولي الأونسيترال UNCITRAL بوضع مشروع قانون التجارة الإلكترونية، واعتمد من الجمعية العامة للأمم المتحدة، وهو ما عرف بالقانون النموذجي للتجارة الإلكتروني، وكان الهدف من هذا القانون هو إيجاد بيئة قانونية آمنة لتيسير استعمال وسائل الاتصال الحديثة، بما يستدعى تعديل الأنظمة القانونية القائمة، وطلبت من الدول تضمينه تشريعاتها الوطنية.

كما قامت العديد من المنظمات الدولية بوضع قواعد ونظم وقرارات منظمة لعمل التجارة الإلكترونية، وسنستعرض في هذا الصدد أعمال لجنة الأمم المتحدة للقانون التجاري الدولي " الأونسيترال "، ثم منظمة التجارة العالمية، ثم أعمال المنظمة العالمية للملكية الفكرية " الوايبو "، وأعمال منظمة التعاون الاقتصادي والتنمية، ثم الاتحاد الأوروبي، وفي النهاية نعرض للمنظمات الإقليمية متعددة الأطراف، وذلك الترتيب التالي:

المطلب الأول: لجنة الأمم المتحدة لقانون التجارة الدولية

المطلب الثاني: منظمة التجارة العالمية

المطلب الثالث: المنظمة العالمية للملكية الفكرية

المطلب الرابع: منظمة التعاون الاقتصادي والتنمية

المطلب الخامس: الاتحاد الأوروبي

المطلب السادس: المنظمات الإقليمية متعددة الأطراف

المطلب الأول

لجنة الأمم المتحدة لقانون التجارة الدولية

اهتمت منظمة الأمم المتحدة ممثلة في لجنة القانون التجاري الدولي الأونسيترال UNCITRAL [1] بوضع مشروع قانون التجارة الإلكترونية، وقد تم لها ذلك في 14 يونيه 1996 واعتمد من الجمعية العامة للأمم المتحدة في الجلسة رقم 162/15 المؤرخة بتاريخ 16 ديسمبر 1996[2]، وهو ما عرف بالقانون النموذجي للتجارة الإلكترونية.

وكان الهدف من هذا القانون هو وضع بيئة قانونية آمنة لتيسير استعمال وسائل الاتصال الحديثة بما يستدعي تعديل الأنظمة القانونية القائمة، ولا يعتبر هذا القانون ملزمًا للدول ما لم تضمنه تشريعاتها الوطنية، مما من شأنه أن ييسر السبل أمام استخدام التجارة الإلكترونية، ويكون مقبولا لدى الدول ذات الأنظمة القانونية والاجتماعية والاقتصادية المختلفة، ويمكن أن يساهم على نحو مهم في تنمية علاقات اقتصادية دولية منسجمة، وذلك بعد أن لوحظ أن عددًا متزايدًا من المعاملات في التجارة الدولية يتم عن طريق التبادل الإلكتروني للبيانات وغير ذلك من وسائل الاتصال التي يشار إليها عادة باسم (التجارة الإلكترونية)، والتي تنطوي على استخدام بدائل للأشكال

---

(1) انظر موقع الأمم المتحدة united National على الإنترنت www.uncitral.org

(2) Dr. Charles Chatterjee E، Commerce law (for Business Managers) , op ,cit. 19

الورقية للاتصال وتخزين المعلومات، وكان اعتماد اللجنة للقانون النموذجي بشأن التجارة الإلكترونية في دورتها التاسعة والعشرين إيمانًا منها بأن ذلك سيساعد على نحو مهم جميع الدول في تعزيز تشريعاتها التي تنظم استخدام بدائل للأشكال الورقية للاتصال وتخزين المعلومات، وعلى صياغة هذه التشريعات في حال عدم وجودها.[1]

وعلى الرغم من أن هذا المشروع يتعلق بالتجارة الإلكترونية إلا أنه لم يضع تعريفًا محددًا لها، واكتفى بتعريف تبادل المعلومات الإلكترونية التي تشمل التجارة الإلكترونية، فعرفها بأنها "نقل المعلومات إلكترونيًا من حاسوب إلى حاسوب آخر باستخدام معيار متفق عليه لتكوين المعلومات".

(1) القرار الذي اتخذته الجمعية العامة للأمم المتحدة بالجلسة العامة 85 في 16 كانون الأول / ديسمبر 1996. الأونسيترال (UNCITRAL) الهيئة القانونية الرئيسية التابعة لمنظومة الأمم المتحدة في مجال القانون الدولي.

The core legal body of the united nations system in the field of international trade law

وهي هيئة قانونية ذات عضوية عالمية متخصصة في إصلاح القانون التجاري على النطاق العالمي منذ ما يزيد على 30 سنة.

A legal body with universal membership specializing in commercial law reform worldwide for over 30 years

مهمة الأونسيترال هي عصرنة ومواءمة القواعد المتعلقة بالأعمال التجارية الدولية.

UNCITRAL"s business is the modernization and harmonization of rules on international business

للمزيد حول ذلك انظر:

- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، قوانين الأونسيترال النموذجية في مجال التجارة الإلكترونية، مرجع سابق، ص 7.
- قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، مطبوعات الأمم المتحدة، نيويورك 2000، ص 17.
- http://www.uncitral.org

وقد رأت اللجنة أن التعريف يغطي كل استعمالات المعلومات الإلكترونية في التجارة والتي يمكن أن يطلق عليها التجارة الإلكترونية[1]، والقانون وإن لم يضع تعريفًا محددًا للتجارة الإلكترونية إلا أنه بين الوسائل المستخدمة في إبرام العقود الإلكترونية، وقد كان ذلك مقصودًا إذ إنه لدى إعداد هذا القانون قررت اللجنة أن تأخذ في الاعتبار عند التطرق إلى الموضوع المعروض عليها مفهومًا موسعًا للتبادل الإلكتروني للبيانات المتصلة بالتجارة، والتي قد يشار إليها عمومًا تحت عنوان التجارة الإلكترونية، بالرغم من وجود إمكانية استخدام عبارات وصفية أخرى.

وبينت المادة (1) من القانون النموذجي نطاق تطبيق هذا القانون Sphere of application بنصها التالي: (ينطبق على أي نوع من المعلومات يكون في شكل رسالة بيانات مستخدمة في سياق أنشطة تجارية) وقد ورد في هامش المادة أنه ينبغي تفسير مصطلح (أنشطة تجارية) تفسيرًا واسعًا على أنه يشمل المسائل الناشئة عن جميع العلاقات ذات الطابع التجاري، سواء أكانت تعاقدية أم لم تكن، وتشمل العلاقات ذات الطابع التجاري المعاملات التالية على سبيل المثال لا الحصر: المعاملة التجارية لتوريد أو تبادل السلع أو الخدمات، اتفاق التوزيع، التمثيل التجاري أو الوكالة التجارية، الوكالة بالعمولة، الكراء، أعمال التشييد، الخدمات الاستشارية، الأعمال الهندسية، منح التراخيص، الاستثمار، التمويل، الأعمال المصرفية، التأمين، اتفاق أو امتياز الاستغلال، المشروعات المشتركة، وغيرها من أشكال التعاون الصناعي أو التجاري، نقل البضائع أو الركاب جوًا أو بحرًا أو بالسكك الحديدية أو بالطرق البرية.

كما ورد بالمادة (2) والخاصة بتعريف المصطلحات Definitions

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص10.

for the purposes تعريفًا لرسالة البيانات Data message بأنها المعلومات التي يتم إنشاؤها أو إرسالها، واستلامها أو تخزينها، بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك على سبيل المثال لا الحصر تبادل البيانات الإلكترونية أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي.

وعرف القانون تبادل البيانات الإلكترونية Electronic data interchange EDI بأنه نقل المعلومات إلكترونيًا من حاسوب إلى حاسوب، أو باستخدام معيار متفق عليه لتكوين المعلومات.

أما نظام المعلومات Information system فتم تعريفه بأنه النظام الذي يستخدم لإنشاء رسائل البيانات أو إرسالها، واستلامها أو تخزينها، أو لتجهيزها على أي وجه آخر.

ومن بين وسائل الإبلاغ التي يشملها مفهوم التجارة الإلكترونية هناك أساليب الإرسال التالية التي تستند إلى استخدام التقنيات الإلكترونية: الإبلاغ عن طريق التبادل الإلكتروني للبيانات (المعرف تعريفًا ضيقًا بوصفه إرسال البيانات من حاسوب إلى حاسوب بصيغة قياسية موحدة)، وبث الرسائل الإلكترونية التي تنطوي على استعمال المعايير المتاحة للعموم أو المعايير المتعلقة بحقوق الملكية، وإرسال نص لا يراعي شكلا محددًا بالوسائل الإلكترونية عن طريق شبكة الإنترنت على سبيل المثال، ولوحظ أيضًا أن مفهوم التجارة الإلكترونية قد يشمل في ظروف معينة استخدام تقنيات مثل التلكس والنسخ البرقي.[1]

ومن الملاحظ أن صياغة القانون النموذجي تشير باستمرار إلى تقنيات

(1) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، مرجع سابق، ص 18.

الإبلاغ الأكثر حداثة، ومنها مثلا التبادل الإلكتروني للبيانات والبريد الإلكتروني، ورغم ذلك فإن المقصود هو أن تطبق المبادئ التي يقوم عليها القانون النموذجي وكذلك أحكامه في سياق تقنيات إبلاغ أقل تطورًا أيضًا مثل النسخ البرقي.

وقد تكون هنالك حالات يمكن فيها لمعلومات رقمية ترسل أولا في شكل رسالة موحدة القياس عن طريق التبادل الإلكتروني للبيانات، أن يبعث بها عند مرحلة معينة من سلسلة الاتصال بين المرسل والمستقبل في شكل تلكس باستخدام الحاسوب أو في شكل نسخة برقية مطبوعة بالحاسوب، وقد تبدأ رسالة بيانات في شكل إبلاغ شفوي ثم تنتهي في شكل نسخ برقي، أو قد تبدأ كنسخ برقي وتنتهي كرسالة من رسائل التبادل الإلكتروني للبيانات.

ومن خصائص التجارة الإلكترونية أنها تشمل رسائل قابلة للبرمجة يتمثل الفرق الأساسي بينها وبين المستندات الورقية التقليدية في برمجتها بالحاسوب، والقصد هو استيعاب هذه الحالات في القانون النموذجي، بالنظر إلى حاجة المستعملين إلى مجموعة متسقة من القواعد لتنظيم طائفة متنوعة من تقنيات الاتصال التي قد تستخدم بشكل قابل للتبادل، وعلى نحو أعم تجدر الإشارة إلى أنه لا يجوز من حيث المبدأ استبعاد أي تقنية من تقنيات الإبلاغ من نطاق القانون النموذجي، نظرًا لأنه قد يلزم استيعاب التطورات التقنية المقبلة.[1]

والملاحظ على مشروع قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية كما ذكرنا آنفًا, عند حديثنا عن التجارة الالكترونية, أنه لم يعرف مصطلح التجارة الإلكترونية، ولكنه اكتفى بتعريف الوسائل

(1) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، مرجع سابق، ص 18.

المستخدمة في إبرام عقود التجارة الإلكترونية، كما أن هذا المشروع كما رأينا قد توسع في سرد وسائل هذه التجارة الإلكترونية، فبالإضافة لشبكة الإنترنت هنالك تقنية الفاكس والتلكس.[1]

وعقب صدور قانون الأونسيترال النموذجي للتجارة الإلكترونية[2] سارعت العديد من دول العالم إلى إصدار قوانين تنظم المعاملات الإلكترونية مسترشدة في ذلك بأحكام هذا القانون، وكانت سنغافورة أول دولة في العالم طبقت القانون النموذجي للتجارة الإلكترونية، حيث أصدرت قانون المعاملات الإلكترونية سنة 1998، ثم تلتها بعد ذلك عدة دول ومنها الولايات المتحدة الأمريكية وإيطاليا سنة 1999، ثم فرنسا وتونس والصين سنة 2000، وأيرلندا سنة 2001، ثم إمارة دبي، مملكة البحرين سنة 2002.

ولقد اهتمت لجنة الأمم المتحدة لقانون التجارة الدولية في وقت مبكر ببحث المشكلات القانونية المتعلقة بالمعالجة الآلية للبيانات التجارية، خصوصًا بعد أن لوحظ أن تشريعات العديد من الدول تتجه إلى التحفظ على استخدام التسجيلات المعلوماتية في مجال الإثبات.[3]

ومن هنا أصدرت اللجنة توصياتها إلى الحكومات والمنظمات الدولية بإعادة النظر في المتطلبات القانونية بشأن التوقيع الخطي وغيره

---

(1) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 11.

(2) يتكون القانون النموذجي The Model Law of Electronic Commerce من سبعة عشر مادة مقسمة إلى جزأين، الجزء الأول عن التجارة الإلكترونية عموما، والجزء الثاني عن التجارة الإلكترونية في مجالات محددة.

(3) تقرير الأمين العام للأونسيترال بعنوان " القيمة القانونية للتسجيلات المعلوماتية " منشور في الكتاب الثانوي الذي تصدره هذه اللجنة، الجزء 13 (1985) ص 365.

من وسائل التوثيق الورقي في المعاملات التجارية، وكذا السماح باستخدام الوسائل الإلكترونية للتوثيق.[1]

وقد قدمت لجنة الأونسيترال مجموعة من الدراسات التي تستهدف من ناحية إزالة العقبات القانونية التي تحول دون الاعتراف بمستندات التعامل الإلكتروني، ومن ناحية أخرى إقرار التكافؤ بين المستندات الإلكترونية والمستندات الورقية، كذلك أعد فريق العمل الذي شكلته اللجنة نموذجًا لعقد تبادل البيانات إلكترونيًا، وأوصت الشركاء التجاريين باستخدامه، كما أوصت الدول الأعضاء في الأمم المتحدة بأن تأخذ في اعتبارها المبادئ التي وضع على أساسها نموذج العقد.

المطلب الثاني

منظمة التجارة العالمية WTO

نشأت منظمة التجارة العالمية بموجب اتفاقية مراكش التي تم التوقيع عليها في 15 أبريل 1994 وذلك من قِبل ممثلي 118 دولة في مدينة مراكش المغربية، وتم إنهاء إجراءات التصديق على إنشائها ودخلت إلى حيز الوجود في أوائل سنة 1995.[2]

إن الهدف الأساسي لمنظمة التجارة العالمية هو المساعدة في سريان وتدفق التجارة بسلاسة وبصورة متوقعة وبحرية, وتقوم المنظمة بذلك عن

(1) وقد اعتمدت الجمعية العامة للأمم المتحدة هذه التوصية في دورتها الأربعين.

(2) www.wto.org

- وتضم منظمة التجارة العالمية 152 عضو من دول العالم, نذكر منها من الدول العربية: الجزائر مملكة البحرين, المملكة المغربية, دولة الكويت, تونس, جيبوتي, جمهورية مصر العربية, دولة قطر, الإمارات العربيّة المتّحدة, المملكة الأردنية الهاشمية, عُمان, المملكة العربية السعودية.

طريق:

- إدارة الاتفاقيات الخاصة بالتجارة.
- التواجد كمنتدى للمفاوضات المتعلقة بالتجارة.
- فض المنازعات المتعلقة بالتجارة.
- مراجعة السياسيات القومية المتعلقة بالتجارة.
- معاونة الدول النامية في المواضيع المتعلقة بالسياسات التجارية من خلال المساعدات التكنولوجية وبرامج التدريب.
- التعاون مع المنظمات الدولية الأخرى.[1]

وبخصوص التجارة الإلكترونية قامت منظمة التجارة العالمية بتوقيع اتفاقيات عديدة[2]، وأصدرت العديد من الدراسات، ومنها الدراسة التي صدرت في مارس 1998، وقد عرفت منظمة التجارة العالمية World Trade Organization التجارة الإلكترونية بأنها "عبارة عن عملية إنتاج وترويج وبيع وتوزيع المنتجات من خلال شبكة الاتصالات وأدواتها مثل التليفون، الفاكس، التبادل الإلكتروني للمعلومات، والبريد الإلكتروني، وشبكة الإنترنت من خلال (WWW) World Wide Web.

وقد حددت المنظمة موقفها الرسمي من التجارة الالكترونية في مؤتمر منظمة التعاون الاقتصادي والتنمية المنعقد في اوتاوا في شهر اكتوبر 1998 حيث اتضح من دور المنظمة أنها لا تسعى لوضع قواعد جديدة خاصة بالتجارة الالكترونية، وإنما تسعى لاستخدام التنظيم القانوني القائم

(1) http://www.marefa.org

(2) كالاتفاق الذي أصدرته المنظمة العالمية للملكية لفكرية WIPO من مقرها في جنيف سنة 1997 بعنوان: 1995 Agreement between the World Intellectual property Organization and World Trade Organization

والمحدد ضمن اتفاقية الجاتس الخاصة بالتجارة واتفاقية التربس والاتفاق الخاص بخدمات الاتصال.[1]

ومنذ ذلك الوقت واصلت المنظمة إعداد الدراسات وبرامج العمل بخصوص التجارة الالكترونية، وقد كان هذا الموضوع واحدا من موضوعات برامج العمل العديدة المتعين التعامل معها او على الأقل اقتراح التعامل معه في مؤتمر سياتل للمنظمة (11/30- 99/12/3) الذي لم يكتب له النجاح في اطلاق جولة جديدة من المفاوضات التجارية الدولية بسبب عوامل كثيرة ابرزها الخلافات الداخلية بين الدول الاعضاء وتمسك التكتلات الدولية بمصالحها الخاصة الى جانب التأثير الحاد والفاعل للجهات والأفراد المناوئين للافرازات السلبية للعولمة وسياسات تحرير التجارة.

ويتضح لنا أن منظمة التجارة العامية اعتبرت التجارة الإلكترونية مجموعة متكاملة من عمليات عقد الصفقات، وتأسيس الروابط التجارية، وتوزيع وتسويق وبيع المنتجات عبر وسائل إلكترونية.[2]

كما نلاحظ أن في تعريف منظمة التجارة العالمية لم يقتصر تعريف التجارة الإلكترونية على شبكة الإنترنت فقط، إذ يمكن أن تتم عقود التجارة الإلكترونية عن طريق المينيتيل Minitel مثلا كما في فرنسا[3] أو

---

(1) جاء ذلك على لسان مديرها العام في ذلك الوقت Renato Roggiero.

(2) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 6.

(3) وخدمة منيتيل هذه تتحقق عن طريق جهاز يحمل الاسم ذاته, وقد شاع استخدامه في فرنسا على نطاق واسع اعتبارًا من منتصف ثمانينيات القرن الماضي، وتتم هذه الخدمة عن طريق جهاز يشبه جهاز الكمبيوتر المنزلي ولكنه صغير الحجم نسبيا, يتكون من شاشة صغيرة ولوحة أزرار تشتمل على الحروف والأرقام مثل تلك المختصة بالكمبيوتر, وهو وسيلة اتصال مرئية لنقل الكتابة على الشاشة دون =

Viditel في هولندا أو Prestel في إنجلترا أو Bildschirmtext في ألمانيا.

ومن هذا التعريف يتضح أن التجارة الإلكترونية تشمل جميع الأنشطة الناشئة عن العلاقات ذات الطابع التجاري سواء أكانت تعاقدية أو لم تكن ويعيب على هذا التعريف أنه قصر الأنشطة على المنتجات فقط دون الخدمات ومن ثم لا يدخل في نطاق التعريف الخدمات الاستشارية مثلا أو منح التراخيص أو الخدمات المصرفية.

المطلب الثالث

المنظمة العالمية للملكية الفكرية WIPO

لقد اهتمت منظمة الوايبو WIPO بالجوانب القانونية للتجارة الإلكترونية، لكنها اهتمت بشكل أكبر بموضوع حماية الملكية الفكرية المرتبطة باستخدام تقنيات المعلومات، خصوصًا في مجال العلامات التجارية وبرامج الكمبيوتر وقواعد البيانات.

وقد وضعت المنظمة العالمية للملكية الفكرية نظامًا لتسوية طائفة من منازعات التجارة الإلكترونية، أهمها تلك المتصلة بأسماء النطاق أو الحقول، وفي هذا الإطار قام مركز التحكيم التابع لهذه المنظمة بتطوير نظام لتسوية المنازعات مباشرة من خلال شبكات الاتصال دون الحاجة للتواجد المادي للأشخاص أو الأشياء[1].

= الصور, أي أنها وسيلة اتصال بواسطة الكتابة، ويكفي لاستعماله أن يوصل بخط التليفون, وقد أخذ مكانة مهمة في عالم الاتصالات والمعلومات، كما استخدم كوسيلة لإبرام العقود. انظر: د. أسامة مجاهد، استخدام الحاسب الآلي في المجال القضائي, مجلة القضاة، عدد يناير، يونيو 1990، ص 61 وما بعدها.

(1) يمكن الاطلاع على هذا النظام من خلال شبكة الإنترنت على الموقع =

وقد انعكس الاهتمام المتزايد للمنظمة بجوانب حقوق الملكية الفكرية المرتبطة بالتجارة الإلكترونية خصوصًا فيما يتعلق بحماية هذه الحقوق من المخاطر التي تتعرض لها عند طرح المصنفات الأدبية والفنية على شبكة الإنترنت، وعلى أعمال المنظمة من مؤتمرات ودورات تدريبية، وأيضًا الدراسات التي تنشرها من حين لآخر[1].

وحيث إن شبكة الإنترنت تحقق توسعًا ملحوظًا متزايدًا، وازدادت قدرتها على نشر المعلومات والمعرفة فقد دفع ذلك المتعاملين إلى نقاش نظام الملكية الفكرية والشكل المستقبلي للعالم في ظل شبكة الإنترنت، والجديد في هذه البيئة أن المعلومات والمعارف متزايدة بصورة تدعو إلى إعمال العقل المبدع في وضع نظام قانوني لحماية الملكية الفكرية، وهو أمر حاسم في الحفاظ على الاستقرار والإنصاف باعتباره الأساس لتنمية المجتمع الرقمي، وسوف يؤدي نظام الملكية الفكرية دورًا حاسمًا في تشكيل العالم الرقمي، وشبكة الإنترنت، ويكون له تأثير عميق على المدى الطويل، وهي تأثيرات واضحة الآن.

وقد بدأت المنظمة الدولية للملكية الفكرية جدول أعمال أنشطة البرنامج الرقمي للوايبو والتي تعكس وتستجيب لتأثير شبكة الإنترنت، والتكنولوجيات الرقمية وأثرها على نظام الملكية الفكرية، وفي الفترة القادمة ولمدة سنوات

= الآتي: www.aribiterwipo.int ورغم اهتمام النظام المذكور بمنازعات أسماء الحقول (النطاق) والعلامات التجارية على وجه الخصوص، إلا أن الخصائص التي تميزه من حيث السرعة وقلة التكاليف تجعله صالحًا لتسوية منازعات أخرى مرتبطة بالتجارة الإلكترونية.

(1) انظر مثلا دراسة منظمة الوايبو تحت عنوان: دراسة مبدئية في التجارة الإلكترونية ومسائل الملكية الفكرية (مايو 2000)، وانظر في هذا الصدد الموقع الآتي: www.wipo.org

ستكون المنظمة ملتزمة بصياغة مناسبة تهدف إلى تشجيع ونشر واستغلال الأعمال الإبداعية والمعارف على شبكة الإنترنت، وكذلك حماية حقوق المبدعين تمشيًا مع التطور المستمر في البيئة الرقمية، وهو حقًا تحدٍّ فريد من نوعه.

والقضايا التي يشملها جدول أعمال البيئة الرقمية والذي يتضمن التحدي وسد الفجوة الرقمية، وتطبيق قانون الملكية الفكرية في المعاملات عبر شبكة الإنترنت، وتأثير شبكة الإنترنت والتكنولوجيا الرقمية على مجالات حق المؤلف والحقوق المجاورة، والعلامات التجارية، وأسماء النطاقات، وبراءات الاختراع، فضلا عن تسوية المنازعات.

تم وضع جدول أعمال المنظمة العالمية للملكية الفكرية الرقمية والذي بدأ في سبتمبر 1999 من قبل المدير العام للمنظمة في المؤتمر الدولي بشأن التجارة الإلكترونية والملكية الفكرية، وتمت الموافقة من جانب الدول الأعضاء في المنظمة العالمية للملكية الفكرية بناءً على اقتراح الجمعية العامة بإنشاء موقع على شبكة الإنترنت مخصص لقضايا التجارة الإلكترونية، ويهدف هذا الموقع إلى إبقاء الجمهور على علم تام بأنشطتها في إطار جدول الأعمال الرقمي، ويقدم معلومات مستفيضة بشأن برامج المنظمة العالمية للملكية الفكرية، كما يمكن إرسال البريد الإلكتروني إلى الأطراف المهتمة، ويهدف الموقع إلى تحقيق الآتي[1]:

1) توسيع نطاق مشاركة البلدان النامية من خلال استخدام المنظمة العالمية للملكية الفكرية وغيرها من وسائل الحصول على المعلومات، والمشاركة في التجارة الإلكترونية.

2) تشجيع إنفاذ معاهدة الوايبو بشأن حق المؤلف، ومعاهدة المنظمة

(1) www.wipo.org

العالمية للملكية الفكرية بشأن الأداء والتسجيل الصوتي (WPPT).

3) تعزيز تعديل الإطار التشريعي الدولي لتسهيل التجارة الإلكترونية.

4) تنفيذ التوصيات الواردة في تقرير المنظمة العالمية للملكية الفكرية وأسماء الحقول على السعي لتحديد الهوية في التوافق بين العالم الحقيقي والعالم الافتراضي، من خلال إنشاء قواعد للاحترام المتبادل، والقضاء على التناقضات بين نظام أسماء المجالات ونظام الملكية الفكرية.

5) وضع مبادئ مناسبة، في الوقت المناسب على الصعيد الدولي، لتحديد ملابسات الملكية الفكرية ومسئولية مقدمي الخدمات على شبكة الإنترنت.

6) تعزيز التكيف مع الإطار المؤسسي لتسهيل استغلال الملكية الفكرية في المصلحة العامة في الاقتصاد العالمي والترابط بين النظم الإلكترونية لإدارة حق المؤلف.

7) استحداث وتطوير التعاون بشأن البراءات على شبكة الإنترنت، مع الأخذ في الاعتبار نظام مدريد واتفاق لاهاي في أقرب وقت ممكن.

8) دراسة منح التراخيص للأصول الرقمية، وإشهار الوثائق الإلكترونية، وإدخال إجراء إصدار الشهادات من المواقع امتثالا لمعايير الملكية الفكرية.

9) دراسة قضايا الملكية الفكرية المتصلة بالتجارة الإلكترونية، ووضع المعايير فيما يتعلق بهذه القضايا.

10) التنسيق مع المنظمات الدولية الأخرى في صياغة المواقف الدولية المناسبة بشأن القضايا التي تؤثر على الملكية الفكرية، ولاسيما صحة العقود الإلكترونية الخاصة بالتجارة الإلكترونية وحقوق الطبع في ظل ظهور تكنولوجيا المعلومات الرقمية الجديدة.

المطلب الرابع

منظمة التعاون الاقتصادي والتنمية OECD

منظمة التعاون الاقتصادي والتنمية OECD[1]، هي منظمة دولية مكونة من مجموعه من البلدان المتقدمة التي تقبل مبادئ الديمقراطية التمثيلية واقتصاد السوق الحر، نشأت في عام 1948 عن منظمة التعاون الاقتصادي الأوروبي والتي يتزعمها الفرنسي روبير مارجولين، للمساعدة على إدارة خطة مارشال لإعادة إعمار أوروبا بعد الحرب العالمية الثانية، وبعد فترة تم توسيعها لتشمل عضويتها بلدانًا غير أوروبية، وفي عام 1960 تم تعديلها لكي تكون منظمة التعاون والتنمية الاقتصادية، وتضم حاليًا (29) عضوًا من الدول الصناعية الكبرى، وقد أدت طبيعة نشاط المنظمة إلى الاهتمام بحماية البيانات والمعلومات، والتركيز على تعزيز التجارة والتقدم الاقتصادي بين الدول الأعضاء.

ولقد كرست المنظمة أعمالها في عام 1998 بشكل رئيس للتجارة الالكترونية، منطلقة من قناعة عبرت عنها اجهزتها مرارا مفادها ان التجارة الالكترونية تتطلب حلولا دولية في مرحلة تنظيمها لأن الحلول المتباينة لا تتفق مع الطبيعية الكونية لهذا النمط من الاعمال، ولان التباين قد يقيم حدودا لا تقبلها التجارة الالكترونية.

وقد عرفت منظمة التعاون الاقتصادي والتنمية التجارة الإلكترونية في تقرير نشرته بأن التجارة الإلكترونية " تتعلق بصورة عامة بجميع أشكال المعلومات التجارية التي تتم بين الشركات أو الأفراد، والتي تقوم على أساس التبادل الإلكتروني للبيانات، سواء كانت مكتوبة Text، مرئية

(1) The Organization For Economic Co Operation and Development

Visual Image أو مسموعة Sound " كما أن مفهوم التجارة الإلكترونية يمتد إلى أبعد من ذلك بحيث يشمل الآثار المترتبة على عمليات تبادل المعلومات والبيانات والمعلومات التجارية الإلكترونية، ومدى تأثيرها على المؤسسات والعمليات التي تدعم وتتحكم في الأنشطة التجارية المختلفة[1].

وكانت المنظمة قد دعت إلى انعقاد المؤتمر العالمي للتجارة الإلكترونية بعنوان (عالم بلا حدود " تحقيق إمكانيات التجارة الإلكترونية العالمية ") في الفترة ما بين 7 - 9 أكتوبر سنة 1998 في مدينة أوتاوا وذلك بالتعاون مع الحكومة الكندية، ويعد هذا المؤتمر الوزاري من أوسع المؤتمرات التي تعرضت للجوانب القانونية المختلفة للتجارة الإلكترونية.

وقد ناقش المؤتمر على مدى يومين مسائل بناء الثقة لدى الزبائن والمستخدمين، وتحديدا معايير وقواعد حماية الخصوصية والبيانات الشخصية المخزنة في النظم والمتبادلة بين شبكات المعلومات، ومسائل امن المعلومات التجارية على الخط وسياسات التشفير لمعلومات وبيانات القطاعين الخاص والعام، ومسائل حماية المستهلك وتحديدا قواعد الاختصاص القضائي وحل المنازعات وحقوق الاعلان على الانترنت والحماية من الانشطة غير القانونية والزائفة، وتناول المؤتمر المسائل التي من شانها ان تجعل التجارة الالكترونية، عبر تنظيمها القانوني المحكم، مشابهة تماما للتجارة التقليدية وما تكرس ضمنها من قواعد كفلت قبولها والثقة فيها، وتناول المؤتمر مسائل الدفع النقدي والتحويلات المالية عبر شبكات الاتصال والانترنت وحماية وسائل الدفع الالكتروني ومسائل العقود الالكترونية والتواقيع الالكترونية والسياسات الضريبية المتصلة بالتجارة

(1) د. خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، مرجع سابق، ص28.

الالكترونية ودور القطاعين العام والخاص في تنظيم اعمال التجارة اللاكترونية، وتوقف المشاركون في المؤتمر امام المتطلبات التقنية للتجارة الالكترونية والخطط والاستراتيجيات اللازم اتباعها في ميدان صناعة التقنية والاتصال وضمان البنية التحتية الآمنة لهذه الانماط من الانشطة المستجدة، وعرج المشاركون على مسائل تعظيم منافع التجارة الالكترونية وتجاوز مشكلاتها عبر الاستراتيجيات الوطنية الشاملة لحماية المعلومات وضمان سلامة وامن الانشطة التجارية، والتنظيم القانوني لمشكلات التسليم المادي للبضائع والتنفيذ المادي للخدمات غير التقينة.

وقد خلص المؤتمر الى اقرار عدد من الاليات وتحديد مناطق الاهتمام القانوني الرئيسة، وشملت التوصيات تكليف المنظمة نفسها بوضع خطط العمل وتكليف المنظمات غير الحكومية والحكومية الدولية لاجراء الدراسات ووضع التصورات وذلك لجهة انفاذ الاعلانات الصادرة عن المؤتمر بشان حماية الخصوصية وأمن الشبكات وحماية المستهلك والموثوقية في التجارة الالكترونية، واتباع السياسات الضريبية التي تمنع اية قيود او اعباء على النشاط التجاري الالكتروني.

ولقد قامت منظمة التعاون الاقتصادي والتنمية بعدة دراسات تناولت الجوانب الاقتصادية والاجتماعية للتجارة الإلكترونية، استعرضت فيها أثرها على الأسواق والأعمال، ودعت إلى الاستفادة من مزاياها.

وقد عقد مؤتمر آخر بشأن الجوانب القانونية للتجارة الإلكترونية عام 1999، واستخلص منه أن التنظيم القانوني لهذه التجارة يجب أن يكون واضحًا ومتماسكًا، وأن يساهم في إيجاد بيئة منافسة تشجع معاملات التجارة الإلكترونية، وأشارت النتائج الصادرة عن المؤتمر كذلك إلى ضرورة حماية المستهلكين، وأيضا حماية الخصوصية خلال معاملات التجارة

الإلكترونية، وضرورة توثيق هذه المعاملات، وقد طالب الوزراء المشاركون في المؤتمر بإلغاء أي تمييز ضد وسائل التوثيق الإلكترونية، وتطوير القوانين التي تعيق ازدهار التجارة الإلكترونية[1].

المطلب الخامس

الاتحاد الأوروبي

تنبه الاتحاد الأوروبي إلى أهمية التجارة الإلكترونية منذ بداية انتشارها في أوروبا والولايات المتحدة، وكان له دور فاعل في تنظيمها وتشجيع التعامل بها على مستوى الاتحاد، حيث قام بوضع برنامج خاص بالنظام التجاري لتبادل البيانات الإلكترونية، وأعد اتفاقًا نموذجيًا أوروبيًا لتبادل البيانات إلكترونيا.[2]

وقد عرف الاتحاد الأوروبي التجارة الإلكترونية بأنها: "الأنشطة التي تتم بوسائل إلكترونية، سواء تمت بين المشروعات التجارية والمستهلكين،

---

(1) د. أحمد شرف الدين، عقود التجارة الإلكترونية، مرجع سابق، ص 46.

(2) الاتحاد الأوروبي هو جمعية دولية للدول الأوروبية تضم 27 دولة، تأسس بناءً على اتفاقية معروفة باسم معاهدة ماسترخت الموقعة عام 1992م، ولكن العديد من أفكاره موجودة منذ خمسينيات القرن الماضي، ومن أهم مبادئ الاتحاد الأوروبي نقل صلاحيات الدول القومية إلى المؤسسات الدولية الأوروبية، لكن تظل هذه المؤسسات محكومة بمقدار الصلاحيات الممنوحة من كل دولة على حدة، لذا لا يمكن اعتبار هذا الاتحاد على أنه اتحاد فيدرالي؛ حيث إنه يتفرد بنظام سياسي فريد من نوعه في العالم، وللاتحاد الأوروبي نشاطات عديدة، أهمها كونه سوقًا موحدة ذات عملة واحدة هي اليورو، كما أن له سياسة زراعية مشتركة وسياسة صيد بحري موحدة.

http://ar.wikipedia.org/wiki/

أو بين كل منهما على حدة وبين الإدارات الحكومية.[1]

ووفقا لهذا التعريف تشمل التجارة الإلكترونية أوامر الطلب الإلكترونية للبضائع والخدمات، والتي يمكن توصيلها بالطرق المعتادة كالبريد أو مندوب الشركات (التجارة الإلكترونية غير المباشرة) أو بطرق التسليم المعنوية للمنتجات والخدمات (التجارة الإلكترونية المباشرة) كبرامج الكمبيوتر والمجلات الإلكترونية وسندات الشحن الإلكترونية والأسهم المالية الإلكترونية.

وقد وضح اهتمام الاتحاد الأوروبي بموضوع التجارة الإلكترونية، حيث جاءت التوجيهات الصادرة منه في هذا المجال واحدًا بعد الآخر كما سبق وأن أسلفنا في بيانها.

حيث قصر التوجيه الصادر في 20 مايو 1997 والمتعلق بحماية المستهلك في العقود المبرمة عن بعد في مادته الثانية تعريفه على العقد الإلكتروني بأنه كل عقد يتعلق بالسلع أو الخدمات يتم بين مورد ومستهلك عن بعد، أو تقديم الخدمات التي ينظمها المورد والذي يتم باستخدام واحدة أو أكثر من وسائل الاتصال الإلكترونية لإتمام العقد[2].

كما عرف التوجيه المشار إليه تقنية الاتصال عن بعد بأنها كل وسيلة دون وجود مادي ولحظي للمورد والمستهلك يمكن أن تستخدم لإبرام العقد بين طرفيه[3].

أما التوجيه الثاني الصادر عن البرلمان الأوروبي رقم 2000-31 في

(1) Ravi kalakota & Andrew B.whinston,Frontiers of electronic commerce. Addison Wesley publishing 1996 p 225.

(2) www.tashreaat.com/view_studies2.asp?id=288std_id=66

(3) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص14.

8 يونيو 2000[1] في شأن بعض الجوانب القانونية لخدمات شركة المعلومات، وبصفة خاصة التجارة الإلكترونية في السوق المحلي، فقد عرف الاتصال التجاري بأنه: "كل شكل من أشكال الاتصال يستهدف تسويق بضائع أو خدمات بصورة مباشرة أو غير مباشرة بين مشروع أو منظمة أو شخص يباشر نشاطًا تجاريا أو صناعيا". وقد حث التوجيه الدول الأعضاء على أن تسمح أنظمتها القانونية بإبرام العقود بالطرق الإلكترونية، وألا تحد من أثرها وفعاليتها لمجرد أنها إلكترونية[2].

والواضح أن هذا التوجيه قد صدر عامًا وشاملا لموضوع التجارة الإلكترونية وأشخاصها، على خلاف التوجيه الأول الذي خص التعاقد عن بعد المتعلق بالبضائع أو الخدمات، على حين أن التوجيه الثاني تحدث عن تسويق البضائع والخدمات والأنشطة التجارية أو الصناعية أو الحرفية أو المهنية بصورة منتظمة، وتضمن التوجيه إشارة للدول الأعضاء بتعديل تشريعاتها كي تستوعب التجارة الإلكترونية ولا تؤثر عليها بصورة سلبية بأن تحد من أثرها أو فاعليتها لمجرد أنها تتم بتقنية إلكترونية[3].

ثم جرت محاولات أخرى في أوروبا لإيجاد إطار عام تلتزم به دول المجموعة الأوروبية أثناء إصدار تشريعاتها الداخلية المتعلقة بتعديل قواعد الإثبات، بما يتماشى مع متطلبات التجارة الإلكترونية، وتم تحديد ثلاثة

---

(1) Directive 2000/31/EC of the European Parliament and of the Council، of 8 June 2000، on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص15.

(3) د. عبد الفتاح مراد، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 37.

محاور في هذا الشأن، الأول بشأن الأثر القانوني للتوقيع الإلكتروني، والثاني يتعلق باعتماد هذا التوقيع والاعتراف المتبادل بين الدول الأعضاء، وتحديد المواصفات التي يتم على أساسها اعتماد التوقيع الإلكتروني، والثالث يتعلق بتحديد التزامات الجهة القائمة على خدمة اعتماد التوقيع الإلكتروني.

وتم تشكيل لجنة لهذا الغرض، ووضعت اللجنة مشروع الإطار المنوط بها إعداده، ومن أهم ملامح هذا المشروع:

1) استلزام الكتابة الورقية في شأن التصرفات القانونية ذات القيمة الكبيرة مع رفع حد حرية الإثبات.

2) وضع النصوص التي تساوي بين المحرر الإلكتروني والمحررات العرفية من حيث القيمة طالما كان التوقيع موثقًا.

3) اعتبار شهادة المصادقة الصادرة من جهة متخصصة تخضع في إنشائها وممارستها لعملها لرقابة الدولة - قرينة بسيطة على صحة المحرر الإلكتروني والتوقيع الوارد به.

وفي 30 نوفمبر 1999 تم إقرار هذا المشروع، وأصبح يسمى باسم التوجيه الأوروبي بشأن المحررات الموقعة إلكترونيًا.

يقودنا الحديث عن الاتحاد الأوروبي للحديث عن مجلس أوروبا The Council of Europe (COE)[1]، والذي تنبه منذ ثمانينيات القرن العشرين إلى ضرورة التنظيم القانوني للمسائل المتصلة بالمعلوماتية, والتصدي للأنشطة الإجرامية والتهديدات المحتملة, وكان ذلك في أكتوبر 1985 حيث تم إعداد الاتفاقية الأوروبية بشأن حماية البيانات الشخصية بالنظر إلى المعالجة الآلية للبيانات.

(1) يتكون مجلس أوروبا من 41 دولة, ولقد تأسس في عام 1949 .http://www.coe.int

وفي 2001/11/23 في بودابست بالمجر Budapest قامت بالتوقيع على الاتفاقية الأوروبية حول الجريمة الافتراضية Convention on cybercrime ثلاثون دولة من أصل 43 دولة من أعضاء مجلس أوروبا، بينها 12 دولة من الاتحاد الأوروبي، بالإضافة إلى كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية.

وتعد هذه الاتفاقية من أهم إنجازات الاتحاد الأوروبي, حيث قام الأوروبيون عند وضعهم للاتفاقية بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي[1] في عام 1997، وذلك بقصد إعداد اتفاقية تتضمن كيفية تسهيل التعاون الدولي في الإجراءات الجنائية في الجرائم الناشئة عن استخدام الحاسوب والإنترنت, وصدر أول مشروع لهذه الاتفاقية في أبريل من العام 2000, ثم تم تعديل هذا المشروع حتى صدر في صورة اتفاقية في عام 2001, علمًا بأن هذه الاتفاقية تسمح للدول غير الأعضاء في الاتحاد الأوروبي بالتقدم بطلب عضوية فيها (المادة 48 من الاتفاقية)[2].

وقد تضمنت هذه الاتفاقية في موضوعها ثلاثة أقسام كبرى، يتناول القسم الأول منها مجموعة الجرائم التي تتعلق بالإنترنت والحاسوب, ويتناول القسم الثاني مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذه النوعية من الجرائم, كما تضمن القسم الثالث موضوع التعاون الدولي بين الدول الأعضاء الموقعين على الاتفاقية, وتكونت هذه الاتفاقية من ثمانية وأربعين مادة, موزعة على أربعة أبواب, يعالج الباب الأول منها المصطلحات, ويتناول الباب الثاني الإجراءات الواجب اتخاذها على المستوى القومي (القواعد الموضوعية والإجرائية والاختصاص القضائي),

(1) Committee of Experts on crime in Cyberspace
(2) www.cybercrime.gov/coedraft.html

أما الباب الثالث فقد تم تخصيصه لدراسة التعاون الدولي, وهو يشتمل على قسمين أولهما المبادئ العامة, والثاني الأحكام الخاصة, وأخيراً يأتي الباب الرابع والذي يتناول أحكامًا ختامية.

وبالاطلاع على القواعد الموضوعية في هذه الاتفاقية نجد أنها نصت على ما يلي:

أولا: الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية:

وقد تناولت المواد من 2 – 6 الجرائم التالية:

1) الدخول غير المشروع (المادة 2).
2) الاعتراض غير المشروع (المادة 3).
3) الاعتداء على سلامة البيانات (المادة 4).
4) الاعتداء على سلامة النظام (المادة 5).
5) إساءة استخدام أجهزة الحاسب (المادة 6).

ثانيًا: الجرائم المعلوماتية (الجرائم المتعلقة بالحاسب):

وقد تناولت المواد 7، 8 الجرائم التالية:

1) التزوير المعلوماتي (المادة 7).
2) الغش المعلوماتي (المادة 8).

ثالثًا: الجرائم المتعلقة بالمحتوى:

ونصت على الجرائم المتصلة بالمواد الإباحية الطفولية (المادة 9).

رابعًا: الجرائم المتصلة بالاعتداءات الواقعة على حقوق الملكية الفكرية والحقوق المجاورة،

حيث نصت عليها (المادة 10).

خامسًا: أشكال أخرى للمسئولية والجزاءات:

وقد تناولت المواد من 11 - 13 ما يلي:

1) أحكام الشروع والمساعدة والتحريض (المادة 11).

2) مسئولية الأشخاص المعنوية (المادة 12).

3) الجزاءات والتدابير (المادة 13).

أما القسم الخاص بالإجراءات فقد تناول ما يلي:

أولا: أحكام عامة:

ويضم المواد 14، 15 وفقا للآتي:

1) مفهوم النصوص الإجرائية (المادة 14).

2) الشروط والإجراءات الوقائية (المادة 15).

ثانيًا: التحفظ على البيانات المعلوماتية المخزنة.

ويضم المواد 16، 17 وفقا للآتي:

1) التحفظ العاجل على البيانات المعلوماتية المخزنة (المادة 16).

2) التحفظ والإفشاء العاجلان لبيانات المرور (المادة 17).

ثالثًا: إصدار الأوامر:

ونصت على الأمر بتقديم بيانات معلوماتية (المادة 18).

رابعًا: البحث ومصادرة بيانات الكمبيوتر المخزنة:

حيث تم النص على تفتيش وضبط البيانات المعلوماتية المخزنة (المادة 19).

خامسًا: تجميع بيانات الحاسب في الوقت الصحيح.

وتناولت المادتان 20، 21 ما يلي:

1) التجميع في الوقت الفعلي للبيانات الخاصة بالمرور (المادة 20).

2) اعتراض البيانات المتعلقة بالمحتوى (المادة 21).

سادسًا: الاختصاص:

حثت الاتفاقية الدول على إقرار إجراءات تحدد الاختصاص القضائي بخصوص الجرائم المقررة في المواد من 2 - 11 من هذه الاتفاقية عند ارتكاب جريمة على: أ- أراضيها, ب- أو على متن السفن التي ترفع علم الدولة , ج- أو الطائرات المسجلة وفقا للقانون, د- بمعرفة أحد مواطنيها (المادة 22).

كما نصت الاتفاقية على التعاون الدولي, والأسس العامة المتعلقة بهذا التعاون الدولي وحالات تسليم المجرمين وتبادل المساعدات, وألزمت الدول الأعضاء بإنشاء نقطة اتصال متاحة على مدار اليوم وطيلة أيام الأسبوع, وذلك لضمان تقديم المساعدات لغرض التحقيقات أو الإجراءات الخاصة بالجرائم المتعلقة بنظم وبيانات الحاسوب, أو لتجميع الأدلة الخاصة بالجريمة في شكل إلكتروني.

والاتفاقية على الرغم من النجاح الكبير الذي حققته - ليس على مستوى الدول الأوروبية فقط وإنما على مستوى دول العالم - إلا أنها واجهت الكثير من النقد، وخاصة من جماعات حقوق الإنسان وبالذات المواد الخاصة بالتحفظ على البيانات, كما انتُقدت الاتفاقية بتحديد عدد قليل فقط من جرائم المعلوماتية وعدم توسعها في التجريم, ونحن نعتقد أن الاكتفاء بهذه الجرائم يعود إلى وجود الأساس القانوني لدى الدول الأوروبية, فالكثير من هذه الدول لديها قوانين تعالج جانبًا من جوانب المعلوماتية[1].

---

(1) النص الأصلي للاتفاقية على الموقع:www.cybercrime.gov/coedraft.html
وانظر أيضا: د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001) والبروتوكول الملحق بها, 2009 ,=

المطلب السادس

المؤسسات الإقليمية متعددة الأطراف

سعت العديد من المؤسسات الإقليمية لتنظيم التجارة الإلكترونية بوضع قواعد منظمة تتصل بعملها، وسوف نتناول في هذا المطلب التنظيم القانوني للتجارة الإلكترونية في المنظمات الإقليمية متعددة الأطراف، وعلى ذلك فإننا سنتحدث عن اللجنة الاقتصادية لأوروبا التابعة للأمم المتحدة، ومنظمة الأسماء والأرقام (الآيكان)، ومنظمة التعاون الاقتصادي لآسيا والمحيط الهادي (أبيك)، وأعمال غرفة التجارة الدولية، ثم نتطرق إلى دور الجامعة العربية في هذا المجال، وذلك على النحو الآتي:

الفرع الأول

اللجنة الاقتصادية لأوروبا التابعة للأمم المتحدة

قامت هذه اللجنة[1] بوضع مجموعة من القواعد المتعلقة بتبادل البيانات إلكترونيًا بهدف توحيد لغة التبادل بين أطراف التعامل في الدول المختلفة، وجرت صياغتها تحت اسم الرسائل النمطية للأمم المتحدة United Nations Standard Message (UNSM)[2].

= وللتعليق على الاتفاقية راجع د. عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، بدون ناشر، 2005، د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، 2003، وللمؤلف نفسه أيضا: اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، 2007.

(1) تغير اسمها سنة 1997 وأصبحت مركز تسيير إجراءات وأعمال الإدارة والتجارة والنقل CEFACT.

(2) وهى تتضمن تعليمات خاصة بالتعاقد، وإخطار الإرسال والوصول، وأمر الشراء،=

ونشير إلى أن هذه اللجنة قامت عام 1995 بإعداد نموذج لعقد تبادل البيانات إلكترونيًا لأغراض الاستخدام التجاري الدولي، وفي إطار جهود هذه اللجنة فقد تم تكليف مجموعة عمل قانونية لمراجعة نموذج العقد المذكور، بما يسمح للاستخدام العام في عمليات التجارة الإلكترونية، على أن يوضع في الاعتبار ما يلي:

أولا: الحاجة إلى اتفاق الشركاء التجاريين على إطار من المبادئ الأساسية للتعامل والتي تتصف بالمرونة لتستوعب الأعمال التجارية اليومية.

ثانيا: أن يستهدف اتفاق التجارة الإلكترونية خدمة أغراض التجارة ومتطلباتها بين أطرافها باستخدام كل أشكال الاتصالات الإلكترونية.

وبعد أن انتقلت اختصاصات اللجنة الاقتصادية لأوروبا إلى المركز الجديد لتيسير الإجراءات والممارسات لأغراض الإدارة والتجارة والنقل، فقد جرى تكوين فريق عمل قانوني دائم ليعالج القضايا القانونية للممارسات والإجراءات القانونية المرتبطة بالتقنيات الجديدة، بما في ذلك التجارة الإلكترونية والتبادل الإلكتروني للبيانات، وبالتالي اقتراح حلول وأدوات عملية للتصدي للعقبات القانونية التي تحول دون استخدام تلك التقنيات، ويتضمن برنامج عمل فريق العمل القانوني - بالإضافة إلى حصر المعوقات القانونية والتجارية الوطنية التي تعوق التجارة الإلكترونية - حماية البيانات، والاختصاص القضائي، وتسوية المنازعات الناشئة في سياق شبكة الإنترنت، وكيفية زيادة الوعي بالقضايا القانونية المرتبطة بالتجارة الإلكترونية والتبادل الإلكتروني للبيانات.[1]

= وجدول مواعيد التسليم، والإخطار الجمركي والاعتماد المستندي.

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراه، كلية =
= الحقوق، جامعة عين شمس، ص 46.

الفرع الثاني

منظمة الأسماء والأرقام الآيكان

تتولى الآيكان ICANN[1] مسئولية تنسيق إدارة العناصر الفنية في نظام أسماء المواقع، وذلك لضمان تيسير تدفق المعلومات على نطاق العالم، بحيث يتسنى لجميع مستخدمي شبكة الإنترنت إيجاد العناوين الصحيحة، وتقوم الآيكان بهذا عن طريق تخصيص أسماء المواقع العليا (ومثال ذلك org. net.com. info).

ويؤدي نظام أسماء المواقع العديد من الخدمات للتجارة الإلكترونية، حيث يجعل من شبكة الإنترنت مصدرًا عالميًا للمساعدة، ومن دون هذه الميزة قد يتطابق اسم الموقع ذاته مع مواقع كثيرة على الشبكة تحت ظروف مختلفة، مما يؤدي إلى وقوع ارتباك في تبادل المعلومات بين أطراف التجارة الإلكترونية على مستوى العالم.

وتعمل الحكومات والمنظمات الدولية المتعاهدة ضمن هيكل الآيكان في شراكة مع مؤسسات الأعمال والمنظمات وأفراد ذوي مهارات عالية ممن لهم دور في بناء شبكة الإنترنت العالمية والمحافظة عليها، ويعالج

(1) هيئة شبكة الإنترنت للأسماء والأرقام المخصصة (الآيكان) منظمة غير ربحية تم تأسيسها دوليا لتتولى مسئولية توزيع مجالات العناوين في بروتوكول شبكة الإنترنت وتخصيص معرفات البروتوكول وإدارة نظام سجلات المواقع العامة عالية المستوى (gTLD) وسجلات المواقع عالية المستوى لرمز الدولة (ccTLD)، كما أنها تضطلع بمسئولية وظائف إدارة نظام الخوادم المركزية، وقد كانت هذه الخدمات تقدم أصلا بموجب عقد حكومي أمريكي من قِبل سلطة تخصيص أسماء شبكة الإنترنت (IANA) وغيرها من الهيئات، أما الآن فتقوم الآيكان بالمهام التي كانت تؤديها السلطة.

المشاركون في الآيكان أية أمور تؤثر بشكل مباشر في مهمة الآيكان الخاصة بالتنسيق الفني، والعمل على الالتزام بمبدأ الحد الأقصى من التنظيم الذاتي في الاقتصاد ذي التقنية العالية لمجتمع شبكة الإنترنت.

ويعمل مجلس إدارة الآيكان والذي يضم جنسيات مختلفة على الإشراف على عملية وضع السياسات، حتى تستطيع أن تؤدي التزامها التشغيلي تجاه مجتمع شبكة الإنترنت، حيث إنها مصممة للاستجابة لحاجات التقنيات والاقتصاديات المتغيرة، وتعمل أكثر من ثمانين حكومة على توفير المشورة لمجلس الإدارة[1]، حتى يمكن توفير الاستقرار والتكامل في شبكة الإنترنت، وهو ما أدى إلى تحقيق الإنجازات الآتية[2]:

- أوجدت الآيكان سوقًا تنافسية لتسجيلات أسماء المواقع العامة عالية المستوى، مما أدى إلى تخفيض تكاليف أسماء المواقع بنسبة 80% مما وفر على المستهلكين والشركات والأعمال ما يزيد عن مليار دولار أمريكي سنويًا من رسوم تسجيل المواقع.
- قامت الآيكان بتنفيذ السياسة الموحدة لحل نزاعات أسماء المواقع (UDRP) حيث تم استخدامها لحل أكثر من 5000 نزاع على حقوق أسماء المواقع.
- وبالتنسيق مع المجتمعات الفنية وأصحاب المصالح المناسبين اعتمدت الآيكان إرشادات خاصة بنشر أسماء المواقع الدولية (IDN)، مما أتاح الفرصة لتسجيل مواقع بمئات اللغات حول العالم.

(1) يضم مجلس الآيكان مواطنين من أستراليا والبرازيل وبلغاريا وكندا والصين وفرنسا وألمانيا وغانا واليابان وكينيا وكوريا والمكسيك وهولندا والبرتغال والسنغال وإسبانيا والمملكة المتحدة والولايات المتحدة الأمريكية.

(2) At: http://www.icann.org

الفرع الثالث

منظمة التعاون الاقتصادي لآسيا والمحيط الهادي

تأسست أبيك APEC[1] من 12 عضوًا على رأسهم الولايات المتحدة الأمريكية الداعم الرئيسي للمنتدى، للتعامل مع منطقة شرق آسيا الشاسعة، وكوسيلة جديدة للتعامل مع الجهة الغربية لأراضيها في فترة ما بعد الحرب الباردة، خاصة وأن روسيا والصين من أعضاء المنتدى، ثم توسع المنتدى ليضم 21 عضوًا حتى نهاية عام 1999[2].

وفي عام 1997 اتفق قادة الدول الأعضاء في المنظمة على وضع خطة عمل للتجارة الالكترونية تكفل تحقيق الدول الاعضاء لمتطلباتها وايجاد اطار قانوني موحد لهذه الغاية، و في عام 1998 وتحديدا في مؤتمر المنظمة المنعقد في كوالالامبور أصدر الاعضاء تصريحا يتضمن الدعوة لاطلاق النشاط التجاري الالكتروني في المنطقة وتطوير صيغ التعاون التقني وبناء البنية التحتية للتجارة الالكترونية والاستثمار في هذا القطاع.

(1) منظمة التعاون الاقتصادي لآسيا والهادي (أبيك Pacific Economic،The Asia)، هو منتدى اقتصادي تأسس عام 1989 كملتقى للتشاور لتعزيز النمو الاقتصادي والتكامل بين الدول التي تطل على المحيط الهادي من جهته الغربية والشرقية.

(2) يضم منتدى أبيك خليطًا من الدول من الناحية الثقافية ومستويات النمو الاقتصادي والازدهار الاجتماعي والأهداف الوطنية والدينية والأوضاع السياسية، فمن الساحل الغربي الآسيوي للمحيط الهادي يضم المنتدى 16 دولة: اليابان وكوريا الجنوبية وروسيا والصين وتايوان وهونغ كونغ والفليبين وبروناي وسنغافورة وإندونيسيا وماليزيا وتايلاند وفيتنام وأستراليا ونيوزيلندا وبابوا غينيا الجديدة، ومن الساحل الشرقي الأمريكي للمحيط يضم خمس دول: الولايات المتحدة الأمريكية وكندا والمكسيك وبيرو وشيلي.

تطورت أهداف وآليات المنتدى بشكل سريع، ويفترض أن تستكمل إجراءات تحرير التجارة والاستثمار وتدفق الأموال والخدمات عبر الشبكة الدولية فيما يعرف بالتجارة الإلكترونية بين دولها الصناعية مع حلول عام 2010 ودولها النامية مع حلول عام 2020، وجاء تأسيس المنتدى استجابة لتزايد التبادل التجاري والرغبة في بناء إقليمية جديدة ترتبط بالمحيط الهادي ككل، مما يعني مزج دول الأمريكتين مع الدول الآسيوية.

اقتصر نشاط المنتدى في السنوات الأولى على تبادل الأفكار والخبرات والتنسيق غير الملزم لبعض المبادرات الفردية، وتركز أبيك على الجانب التجاري وفتح فرص جديدة لشعوب المنطقة، خصوصًا في مجال التبادل التجاري عبر التجارة الإلكترونية.

وتعمل أبيك على التركيز على دور القطاع الخاص أكثر من دور الدول، ويجتمع كبار رجال المال والأعمال سنويًا في ظل ما يعرف بمجلس أبيك لتقديم المقترحات والاستشارات المتعلقة بالتجارة الإلكترونية، ويقدم مقترحاته لرؤساء ووزراء دول المنظمة للاستعانة بها في اتخاذ القرارات.

وتعمل منظمة التعاون الاقتصادي لآسيا والمحيط الهادي أبيك على اتخاذ إجراءات تحرير التجارة، أو تحرير قطاع تجاري معين بين دولتين من أعضائها.

الفرع الرابع

غرفة التجارة الدولية

شاركت غرفة التجارة الدولية ICC[1] مع مؤسسات دولية أخرى

(1) أسست غرفة التجارة الدولية ICC في عام 1919 بهدف عام ما زال قائما دون تغيير ألا وهو خدمة قطاع الأعمال الدولي عن طريق تعزيز التجارة والاستثمار، =

معنيـة بشئون التجارة في وضع قواعـد السـلوك الموحـدة لتبـادل البيانـات التجاريـة باسـتخدام الوسائل الإلكترونية عن بعد، وتعالج هذه القواعد بشكل عـام المتطلبات الأساسـية ذات الطـابع التقني والإجرائي مثل أنمـاط تبـادل البيانات وتسجيلها وتخزينها.

وقد كان الهدف من توحيد القواعد المذكورة هـو التوصـل إلى نمـوذج نمطـي لاتفاقيـات أو نظم تبادل البيانـات إلكترونيًا تختـار الأطـراف المعنيـة مـن نصوصـه مـا تـراه مناسـبًا لتحقيـق أهـداف علاقتهم، لكن عندما اتضح أن الفكرة التي يقوم عليها هـذا النمـوذج غـير عمليـة أمـام تنوع متطلبات مستخدمي هذا التعامل اتجهت الغرفة إلى العمل في مشروع التجارة الإلكترونيـة الذي توزعت أعماله بـين ثلاثـة فـروع وهـي: ممارسـات التجـارة الإلكترونيـة، وأمـن المعلومـات، والمصطلحات القانونية.

ويعد دليل التجارة الالكترونيـة الصـادر عـن الغرفـة أحـد أهـم الأدلـة الشـاملة التـي تتـيح مساعدة فاعلة في ميدان الانشطة التشريعية والتنظيمية اللازمة

= وفتح الأسواق للسلع والخدمات والتدفق الحر لرأس المال، ويعـود الفضـل في قـوة الـدفع الأولى لجهـود الغرفة لرئيسها الأول "إتيان كليمنتل" وهو وزير تجارة فرنسي سابق، وبفضل ما كان يتمتع به من نفـوذ تم تأسيس الأمانة العامة للغرفة في باريس، وكان دوره محوريا في إنشاء محكمة التحكيم الدولية التابعة للغرفة في عام 1923, وقد ذاع صيت الغرفة بحيـث تخطـى مرحلـة الاعـتراف بهـا منـذ تلـك الأيـام التـي أعقبت الحرب عندما اجتمع قادة قطاع الأعمال من دول الحلفاء لأول مرة في مدينة أتلانتك، وقد ضمت النواة الأولى للغرفة ممثلين من القطاع الخاص في بلجيكا وبريطانيا وفرنسا وإيطاليـا والولايـات المتحـدة، ثم توسعت لتصبح منظمة أعمال دولية تضم في عضويتها آلاف الشركات والهيئـات في حـوالي 130 بلـدًا. ويوجد من بين الأعضاء عدد كبير مـن الشركات الأكـثر نفـوذا في العـالم وتمثـل كـل القطاعـات الصـناعية والخدماتية.

للتجارة الالكترونية. وقد تعزز هذا الدليل بصدور العديد من الادلة الأكثر تخصصا والمكملة له كالدليل الخاص بالانشطة الاعلانية على الانترنت.

وقد جاء في دراسة للأونكتاد UNCTAD[1] في هذا الشأن أن الفريق العامل المعني بالممارسات التجارية الإلكترونية قد وضع مجموعة من القواعد الأساسية لتنظيم جوانب من التجارة الإلكترونية وتسوية منازعاتها، استهدف بها الاستجابة لمتطلبات تقنيات الاتصال واستخداماتها في إنجاز المعاملات، أما الفريق العامل المعني بأمن المعلومات فقد أعد مجموعة من المبادئ التوجيهية لتعزيز قدرة مجتمع الأعمال الدولي على إبرام صفقات رقمية مأمونة " العرف العام في التجارة الدولية المؤمنة رقميًا "، وتحدد هذه المبادئ التوجيهية إطارًا عامًّا لتأمين الرسائل الرقمية والتصديق عليها، وتنطبق هذه المبادئ على استخدام الترميز بالمفتاح العام لأغراض التوقيعات الرقمية.

أما الفريق العامل المعني بالمصطلحات الإلكترونية فيقوم باستحداث خدمة جديدة في غرفة التجارة الدولية، وذلك باستخدام مستودع إلكتروني مركزي للمصطلحات القانونية، والتي يمكن لذوي الشأن استخدامها في المعاملات الإلكترونية، وسوف يشمل المستودع جميع الأدوات اللازمة لتكوين العقود الإلكترونية.[2]

---

(1) أسس مؤتمر الأمم المتحدة للتجارة والتنمية "الأونكتاد" بناءً على قرار الجمعية العامة رقم 1940 في الدورة 19، وهدف هذه المنظمة دعم التجارة والتنمية الدوليتين, وقد تم إجراء هذه الدراسة في 1998/5/15.

(2) د. أحمد شرف الدين، عقود التجارة الإلكترونية، مرجع سابق، ص 47.

الفرع الخامس

دور الجامعة العربية

اتخذ المجلس الاقتصادي والاجتماعي لجامعة الدول العربية قراره رقم 1317 بتاريخ 17 فبراير 1997 بالإعلان عن إقامة منطقة تجارة حرة عربية كبرى خلال مدة عشر سنوات بدءًا من 1 يناير 1998، ووافق المجلس في القرار نفسه على البرنامج التنفيذي لإقامة هذه المنطقة، متضمنًا الأسس والقواعد والآليات التنفيذية، والبرنامج الزمني للتخفيض في الرسوم الجمركية والضرائب ذات الأثر المماثل المفروضة على كافة السلع العربية ذات المنشأ الوطني المتبادلة بين الدول العربية الأعضاء في منطقة التجارة الحرة العربية.

وكان مؤتمر القمة العربية المنعقد في القاهرة بتاريخ 23/7/ 1996 قد كلف المجلس الاقتصادي والاجتماعي بالإسراع بإقامة منطقة التجارة الحرة العربية، وشكل قرار القمة العربية المظلة السياسية لتبني المجلس الاقتصادي والاجتماعي لقراره بإقامة منطقة التجارة الحرة العربية.

ثم ظهرت بعد ذلك فكرة إقامة منطقة التجارة الحرة العربية الكبرى، وهي عبارة عن اتفاق بين الدول العربية التي وافقت على التبادل الحر فيما بينها وفقًا لاتفاقية محددة البنود "اتفاقية تنمية وتيسير التبادل التجاري بين الدول العربية" ووفقًا لبرنامج زمني محدد "البرنامج التنفيذي لمنطقة التجارة الحرة العربية الكبرى" الذي يقضي بالتخفيض التدريجي للرسوم الجمركية والرسوم والضرائب ذات الأثر المماثل على مدار عشر سنوات (من 1998 حتى 2007)[1].

---

(1) قامت خمسة عشر دولة بتطبيق البرنامج التنفيذي لمنطقة التجارة الحرة العربية =

وقد تعرضت منطقة التجارة الحرة العربية الكبرى إلى بعض المشكلات في بدايتها، وهذا يعتبر أمرًا طبيعيًا مثلها مثل باقي التكتلات الاقتصادية في العالم، حيث كانت القوائم السلبية كثيرة جدًا (استثناء بعض السلع من التخفيض التدريجي نظرًا لظروف وطبيعة تلك السلع ووفقًا لمعايير محددة) ولمدة سنتين فقط منذ سبتمبر 1999 وحتى سبتمبر 2001، وأصبح الآن لا يوجد أي استثناءات بين الدول العربية، وجدير بالذكر أن المجلس الاقتصادي والاجتماعي اتخذ قراره بناءً على رغبة الزعماء العرب يتضمن تقليص المدة الزمنية لتنفيذ منطقة التجارة الحرة العربية الكبرى لتنتهي في الأول من يناير عام 2005، حيث لا يكون هناك رسوم جمركية بين الدول العربية للتبادل التجاري.

وصدر قرار من مجلس جامعة الدول العربية على مستوى القمة بعمان 2001 يقضي بضرورة الإزالة الفورية للقيود غير الجمركية الإدارية والفنية والمالية والنقدية والكمية، وإخضاع كافة الرسوم والضرائب ذات الأثر المماثل للتخفيض التدريجي المتفق عليه، وتعديل القوانين والتشريعات التي تتعارض مع أحكام اتفاقية تيسير وتنمية التبادل التجاري بين الدول العربية وبرنامجها التنفيذي.

وتقوم الآن الأمانة العامة بالعمل على تحرير تجارة الخدمات من خلال اللجان الفنية التابعة للمجلس الاقتصادي والاجتماعي والمجالس الوزارية الأخرى المعنية بالأمر.

= الكبرى، وأعلنت الجمهورية الجزائرية أنها ستدخل حيز التطبيق بعد الانتهاء من الإجراءات التي تمكنها من التطبيق، والدول الأعضاء هي: الأردن، الإمارات، البحرين، الجزائر، السعودية، سوريا، السودان، العراق، عمان، فلسطين، قطر، الكويت، لبنان، ليبيا، مصر، المغرب.

وتولي الأمانة العامة اهتمامًا كبيرًا لميكنة الموضوعات الخاصة بمنطقة التجارة الحرة العربية الكبرى، حيث شكلت لجنة دائمة تعمل في إطار المجلس الاقتصادي والاجتماعي معنية بالمعلومات وتبسيط الإجراءات، قامت تلك اللجنة بالاطلاع على كافة النظم المستخدمة من خلال المصالح الجمركية في الدول العربية بغية الوصول إلى نظام جمركي عربي وموحد، حيث وجدت اللجنة صعوبات جمة في عملية التحليل نظرًا لاختلاف طبيعة كل مصلحة جمركية، ولكن توصلت اللجنة إلى ما يلي:

1) ضرورة ميكنة نموذج الترانزيت العربي الموحد الذي قامت الأمانة العامة بإعداده ووافق عليه المجلس الاقتصادي والاجتماعي، وبالفعل قامت اللجنة - من خلال فريق عربي تقني في مجال البرمجيات منبثق عنها - بإعداد نظام إلكتروني لنموذج الترانزيت العربي الموحد على شبكة الإنترنت بلغة v.basic & sql، ويهدف هذا النظام إلى تسهيل عملية الترانزيت بين الدول العربية.

2) الوصول إلى نموذج جمركي عربي موحد يتم من خلال التخليص الجمركي للسلع المتبادلة إلكترونيًا من خلال شبكة الإنترنت.

3) قامت الأمانة العامة بإعداد موقع على شبكة الإنترنت خاص بمنطقة التجارة الحرة العربية الكبرى، يربط هذا الموقع كافة المواقع الخاصة بالمصالح والهيئات والدواوين الجمركية في العالم العربي، كما يتضمن مجموعة قواعد بيانات منها قاعدة التعريفة الجمركية بثلاث لغات العربية والإنجليزية والفرنسية لكافة السلع مصنفة وفقا للنظام المنسق للسلع HS.CODE على مستوى ثماني أرقام، حيث يمكن من خلال هذه القاعدة الاستعلام عن رمز السلعة أو اسم السلعة لمعرفة كافة بيانات التعريفة الجمركية في كافة الدول العربية

الأعضاء بمنطقة التجارة الحرة العربية الكبرى، كما يحتوي الموقع على مجموعة أخرى من قواعد البيانات منها بيانات المصدرين والمستوردين في الدول العربية، وكذلك قواعد بيانات إحصائية وقواعد بيانات خاصة بقرارات المجلس الاقتصادي والاجتماعي ولجانه الفنية (السادة مدراء الجمارك، ولجنة المعلومات الجمركية، ولجنة التنفيذ والمتابعة والمفاوضات التجارية....الخ)

ومما سبق ذكره عن مجهودات الأمانة العامة لجامعة الدول في هذا المجال، وعن منطقة التجارة الحرة العربية الكبرى، وعن اللجان الفنية التي تدور في فلكها، يتبين الدور الإيجابي الذي تقدمه الأمانة العامة في تيسير التبادل الإلكتروني للمعلومات بصفة عامة، والتجارة العربية البينية بصفة خاصة من خلال العمل على تبسيط الإجراءات وميكنة النماذج الموحدة للتخليص الجمركي للسلع العربية.[1]



(1) د. رأفت عبد العزيز غنيم، دور جامعة الدول العربية في تنمية وتيسير التجارة الإلكترونية بين الدول العربية، نوفمبر 2002، ص 11. بحث منشور على الموقع التالي:
www.ebi.org.eg/E.../Role%20of%20Arab%20League%20in%20development%2...

المبحث الثاني

التجارة الإلكترونية ومجتمع المعلومات

القمة العالمية لمجتمع المعلومات هي قمة لزعماء العالم الملتزمين بتسخير إمكانيات الثورة الرقمية في تكنولوجيا المعلومات والاتصالات لخدمة البشرية، وهي تمثل عملية تعددية حقيقية لأصحاب المصلحة الذين يشملون الحكومات والمنظمات الدولية الحكومية، والمنظمات غير الحكومية، والقطاع الخاص، والمجتمع المدني، وهدف القمة هو بناء مجتمع معلومات جامع يتجه نحو التنمية، مجتمع يستطيع كل فرد فيه استحداث المعلومات والمعارف والنفاذ إليها واستخدامها وتقاسمها، ويتمكن فيه الأفراد والمجتمعات والشعوب من تسخير كامل إمكانياتهم للنهوض بتنميتهم المستدامة لتحسين حياتهم[1].

ووفقًا للقرار 56/183 للجمعية العامة للأمم المتحدة تم تنظيم القمة العالمية من مرحلتين)جنيف 12-10 ديسمبر 2003، وتونس 16- 18 نوفمبر 2005)، وكُلّف الاتحاد الدولي للاتصالات[2] بأداء الدور الرائد في

(1) At: http://www.un.org/arabic/conferences/wsis/

(2) الاتحاد الدولي للاتصالات هو وكالة الأمم المتحدة الرائدة في مسائل تكنولوجيا المعلومات والاتصالات، ويتمثل دور الاتحاد - بوصفه النقطة المركزية العالمية للحكومات والقطاع الخاص - في مساعدة العالم على الاتصال، ويضم ثلاثة قطاعات رئيسية هي الاتصالات الراديوية، تقييس الاتصالات، تنمية الاتصالات، كما ينظم الاتحاد مناسبات التليكوم، وكان الوكالة الرائدة لتنظيم القمة العالمية لمجتمع المعلومات، ويوجد مقر الاتحاد الدولي للاتصالات في جنيف بسويسرا، ويضم في عضويته 191 دولة عضوًا، فضلا عن أكثر من 700 عضو من أعضاء القطاعات والمنتسبين.

http://www.itu.int/net/home/index.ar.aspx

الأعمال التحضيرية بالتعاون مع الجهات المهتمة الأخرى من المنظمات والشركاء.

وسوف نتناول هذا المبحث وفق ثلاثة مطالب كما يلي:

المطلب الأول: القمة المعلوماتية وتنظيم التجارة الإلكترونية

المطلب الثاني: مراحل قمة المعلومات العالمية

المطلب الثالث: الشراكة المجتمعية وتنظيم التجارة الإلكترونية

المطلب الأول

القمة المعلوماتية وتنظيم التجارة الإلكترونية

حدث تحول جذري من المجتمع الصناعي إلى المجتمع القائم على المعلومات أو ما يعرف بثورة المعلومات، وقد أثرت تلك الثورة المعلوماتية على الطريقة التي يعيش بها الناس، وعلى الطريقة التي تتفاعل بها الحكومات مع المجتمع المدني، وتعد المعلومات أداة قوية لتحقيق التنمية الاقتصادية والاجتماعية، وقد وفرت تلك القمة فرصة فريدة لجميع العناصر الفاعلة الأساسية للإسهام بشكل إيجابي في القضاء على الهوة الرقمية وهوة المعرفة، كما أقرت المرحلة الأولى للقمة في جنيف إعلانًا للمبادئ وخطة للعمل وضعتها الحكومات والمؤسسات وجميع قطاعات المجتمع المدني موضع التنفيذ، للتعامل مع التحديات الجديدة لمجتمع المعلومات دائم التطور، وخصوصًا تلك المتعلقة بالتعرف على الطرق التي من شأنها المساعدة على سد الهوة بين الأغنياء والفقراء من حيث الوصول إلى المعلومات العالمية وشبكات الاتصال.

وقد خلق "الانقسام الرقمي" فجوة في المعارف بين الشعوب الغنية بالمعلومات وتلك التي تفتقر إليها، مما قد يمهد السبيل لظهور أشكال جديدة

من "الأمية"، ويعزز الانقسام الرقمي الافتقار إلى المعلومات والمعرفة، ويحدد فرص النمو الاقتصادي وتوزيع الثروة، وتشجع تكنولوجيا المعلومات والاتصال على إقامة "شبكات" اقتصادية واجتماعية من الأفراد والمجتمعات، وتتمثل قوة تلك الشبكات في قدرتها على الربط بين المجموعات المتنوعة عن طريق السماح لها بالوصول إلى المعلومات والمعارف الجوهرية لتحقيق تنميتها الاقتصادية والاجتماعية وتبادل تلك المعلومات والمعارف.

ويستفيد التجار وأصحاب الأعمال والمشروعات من تكنولوجيا المعلومات والاتصال من خلال الفرص التي تهيئها للنهوض بأعمالهم وطنيًا وإقليميًا ودوليًا، وعلاوة على ما تقدم فإن تكنولوجيا المعلومات والاتصال تتيح الفرصة لتقديم الخدمات الأساسية في مجالي الصحة والتعليم على نحو أكثر كفاءة، حيث يمكن للناس الوصول إليها من داخل مجتمعاتهم.

وتؤدي الثورة الرقمية إلى نشوء أشكال جديدة تمامًا من التفاعل الاجتماعي والاقتصادي وقيام مجتمعات جديدة داخل فضاء سيبراني، وعلى عكس الثورة الصناعية التي شهدها القرن المنصرم، فإن ثورة تكنولوجيا المعلومات والاتصال من شأنها الانتشار بشكل سريع والتأثير في حياة الجميع، وتتميز تلك الثورة بقوة تكنولوجيا المعلومات والاتصالات بما يسمح للناس بالوصول إلى المعلومات والمعرفة الموجودة في أي مكان بالعالم في اللحظة نفسها تقريبًا.

وقد سعت قمة المعلوماتية عبر المرحلتين إلى تبني المؤسسات لتكنولوجيا المعلومات والاتصالات، وأن تلعب دورًا أساسيًا في تحقيق النمو الاقتصادي وزيادة الإنتاجية الناتجة عن الاستثمارات وزيادة التجارة وتحسين فرص العمل، بالمشاركة بينها وبين الحكومات والقطاع الخاص لتعزيز قدراتها، مع العمل على وضع السياسات اللازمة والأطر القانونية

والتنظيمية الضرورية لرعاية إقامة المشروعات، وخاصة للمؤسسات المتوسطة الحجم والصغيرة والمتناهية الصغر.

كما طالبت بالنفاذ الشامل دون تمييز إلى تكنولوجيا المعلومات والاتصالات لجميع البلدان، وبضرورة مراعاة مستوى التنمية الاجتماعية والاقتصادية لكل بلد، واحترام نواحي مجتمع المعلومات ذات التوجه التنموي، وحرصت على سد الفجوة الرقمية لكي يمكن بلوغ الأهداف والغايات الإنمائية المتفق عليها دوليًا، وجهود التعاون الدولي في بناء مجتمع المعلومات، مع إقامة أنظمة عامة للمعلومات بشأن القوانين والقواعد، لاستفادة الجميع من المزايا التي تتيحها تكنولوجيا المعلومات والاتصالات للتنمية.

وحرصت القمة المعلوماتية على تطوير مجتمع المعلومات لتحقيق الاحتياجات الخاصة لشعوب البلدان النامية، والبلدان التي تمر اقتصادياتها بمرحلة تحول، والبلدان الأقل نموًا، والبلدان الفقيرة المثقلة بالديون، والأراضي الواقعة تحت الاحتلال.

وتعد من أهم قرارات قمة المعلوماتية تلك الدعوة إلى تطوير نظام تجارة عالمي متعدد الأطراف، يقوم على الشراكة بين الحكومات والقطاع الخاص والمجتمع المدني والأوساط العلمية والأكاديمية والمستخدمين لمختلف التكنولوجيات، على أساس حكم القانون والانفتاح وعدم التمييز والإنصاف وحفز التنمية على نطاق العالم، مما يؤدي إلى شمول مجتمع المعلومات لجميع الشعوب من خلال تطوير واستعمال اللغات المحلية في تكنولوجيا المعلومات والاتصالات.

هذا وقد تطرقت قمة المعلوماتية لمجموعة من القضايا التي تمثل الأسس الجوهرية لمجتمع المعلومات, والتي تمس بصفة مباشرة المجتمع المدني,

ومن هذه القضايا:

- مسألة حقوق الإنسان وحرية التعبير.
- موضوع الملكية الفكرية، حيث إنها تمثل عنصرًا مهمًا في تشجيع الابتكار والإبداع في مجتمع المعلومات.
- إدارة شبكة الإنترنت.
- التنوع الثقافي والبعد الأخلاقي لمجتمع المعلومات.
- التعاون الدولي لتمويل ردم الفجوة الرقمية.

وقد أثبتت الدراسات أن تكنولوجيا المعلومات لها قدرة كبيرة على تحقيق كل هدف من أهداف قمة المعلومات دون استثناء، فالتكنولوجيا تساعد على اختصار المسافات، وتنمية الاقتصاد الجديد (الاتصالي واللامادي)، وتوظيف تطبيقات شبكة الإنترنت في الصحة والثقافة والتعليم، وقد أكدت بعض الاستنتاجات أن الطفل الذي يتعلم بالاعتماد على الحاسوب يكسب في أقصر وقت أضعاف ما يحصل عليه أترابه، وفي الواقع فإن البلدان المصنعة هي التي أقبلت قبل غيرها على توظيف تكنولوجيا الاتصال في تنمية الاقتصاد الجديد.

المطلب الثاني

مراحل قمة المعلومات العالمية

انعقدت القمة العالمية لبناء نظام المعلومات وتشجيع التجارة الإلكترونية لتتسع وتشمل كافة المناطق الدولية دون فواصل جغرافية، ودون تفرقة بين السلع والخدمات، مستندة في ذلك إلى مشاركة الدول (المتقدمة والنامية) والحكومات والقطاع الخاص، مستهدفة تنمية مستدامة من خلال هذا المجتمع المعلوماتي، آخذة في الاعتبار الفئات الفقيرة والمهمشة في الريف

والحضر دون تفرقة، وقد تمت هذه القمة على مرحلتين؛ لذا فإننا سنتناول مراحل القمة على فرعين: مرحلة جنيف 2003 فرع أول، ومرحلة تونس 2005 فرع ثان.

الفرع الأول

المرحلة الأولى جنيف 2003

اجتمع ممثلو شعوب العالم في جنيف من 10 إلى 12 ديسمبر 2003 للمرحلة الأولى من القمة العالمية لمجتمع المعلومات[1]، وتم إعلان الرغبة المشتركة فيما بينهم والالتزام المشترك لبناء مجتمع المعلومات الذي يستهدف التنمية المستدامة للمجتمع، بحيث يستطيع كل فرد فيه استحداث المعلومات والمعارف والنفاذ إليها واستخدامها وتقاسمها، ويتمكن فيه الأفراد والمجتمعات والشعوب من تسخير كامل إمكانياتهم للنهوض بتنميتهم ولتحسين نوعية حياتهم، وذلك انطلاقًا من مقاصد ومبادئ ميثاق الأمم المتحدة، والتمسك بالاحترام الكامل للإعلان العالمي لحقوق الإنسان، وتم في هذه المرحلة إعلان المبادئ العامة التي وافق عليها المجتمعون، وتضمنت هذه المبادئ ما يلي[2]:

(1) حضر مرحلة جنيف من القمة العالمية وفود رفيعة المستوى من 178 بلدًا تشمل رئيس ونائب رئيس 50 دولة وحكومة، وشارك أكثر من 11000 شخص في القمة العالمية والأنشطة المتصلة بالقمة، واعتمد زعماء العالم المجتمعون في مرحلة جنيف من القمة العالمية في 12 ديسمبر 2003 إعلان مبادئ القمة وعنوانه "بناء مجتمع المعلومات: تحدٍ عالمي في الألفية الجديدة". وهذا الإعلان يضع أسس مجتمع المعلومات الناشئ، وتضع خطة عمل القمة التي أيدتها قمة جنيف أهدافًا مرتبطة بمواعيد زمنية لترجمة مجتمع المعلومات الجامع والمنصف من رؤية إلى واقع عملي.

(2) http://www.itu.int/wsis/indexar.html

1) بناء مجتمع المعلومات وفقًا لرؤية مشتركة والتزام مشترك يعد هو التحدي العالمي في الألفية الجديدة.

2) ضرورة تسخير إمكانيات تكنولوجيا المعلومات والاتصالات للنهوض بأهداف التنمية المستدامة، وإقامة شَراكة عالمية من أجل تحقيقها.

3) التأكيد على أن حرية الرأي والتعبير كما وردت في المادة 19 من الإعلان العالمي لحقوق الإنسان هي أساس مجتمع المعلومات، الذي يعطي لكل فرد الحق في الحصول على المعلومات وإذاعتها بأية وسيلة كانت دون تقيد بالحدود الجغرافية، فالاتصال يعد أساس كل تنظيم اجتماعي، وهو محور مجتمع المعلومات، وينبغي أن تتاح فرصة المشاركة لكل فرد في كل مكان، ولا ينبغي استبعاد أحد من الفوائد التي يقدمها مجتمع المعلومات.

4) التأكيد على عدم خضوع الفرد في ممارسته لحقوقه وحرياته لأي قيود إلا ما يقرره القانون، لضمان الاعتراف بحقوق الغير وحرياته واحترامها، ولتحقيق المقتضيات العادلة للنظام العام والمصلحة العامة والأخلاق في مجتمع ديمقراطي يعمل على النهوض بمجتمع للمعلومات تحترم فيه كرامة البشر.

5) التأكيد على دعم مبدأ المساواة في السيادة بين جميع الدول في التعامل مع مجتمع المعلومات باعتباره حصيلة خطوات التقدم العلمي والتقني التي تحققت بفضل تبادل نتائج البحوث.

6) التأكيد على أن المعرفة هي أساس تكنولوجيا المعلومات والاتصالات، وهي تؤثر في بلوغ مستويات أرفع من التنمية، وتذليل العديد من العقبات التقليدية، واختصار الزمن والمسافات، وتجعل من الممكن تسخير إمكانيات هذه التكنولوجيات لصالح الملايين من الناس في

جميع أرجاء المعمورة.

7) تعد تكنولوجيا المعلومات والاتصالات أدوات وليست غاية، فهي وسيلة لزيادة النمو الاقتصادي وخلق فرص العمل وتعزيز الحوار بين الناس والأمم والحضارات.

8) التأكيد على سد الفجوة الرقمية بين البلدان المتقدمة والبلدان النامية، لتحقيق المساواة والمقدرة في استخدامها.

9) التأكيد على اعتبار أن مجتمع المعلومات هو للجيل الحاضر وللأجيال المقبلة، لذا وجب تمكين الشباب والأطفال من التعلم والمساهمة في هذا المجتمع.

10) التأكيد على أن بناء مجتمع المعلومات يأخذ في اعتباره الفئات المهمشة والضعيفة في المجتمع، بما في ذلك المهاجرون والأشخاص المشردون داخليًا واللاجئون، والعاطلون عن العمل، والأقليات وذوو الاحتياجات الخاصة، والفقراء، وخاصة الذين يعيشون في المناطق النائية والريفية وفي المناطق الحضرية.

11) التأكيد على أن بناء مجتمع المعلومات يتطلب أشكالا جديدة من التضامن والشراكة والتعاون بين الحكومات وأصحاب المصلحة الآخرين، من القطاع الخاص والمجتمع المدني والمنظمات الدولية.

12) التأكيد على أن هذا الإعلان لا ينتقص من أحكام ميثاق الأمم المتحدة والإعلان العالمي لحقوق الإنسان، أو من أي صك دولي آخر أو قوانين وطنية.[1]

---

(1) اجتمع ممثلو الحكومات العربية في المؤتمر العربي رفيع المستوى بمدينة القاهرة، وذلك للتحضير لمؤتمر القمة العالمية لمجتمع المعلومات في الفترة من 16: 18 يونيو "حزيران" 2003، وحضر المؤتمر 19 دولة عربية، كما حضر عدد 9 =

هذا وقد جاء في خطة العمل الخاصة بالقمة العالمية لمجتمع المعلومات والصادرة عن الأمم المتحدة[1] بتاريخ 12 ديسمبر 2003 فيما يختص بالتجارة الإلكترونية ما يلي:

= دول إفريقية كمراقب، وأمين عام الاتحاد الدولي للاتصالات، وعدد من الشخصيات المرموقة عالميًا في مجال الاتصالات والمعلومات، بالإضافة إلى ممثلي المنظمات الدولية والإقليمية وممثلي القطاع الخاص والمجتمع المدني، واتخذوا عددًا من القرارات المهمة، ومن أهم ما يعنينا هنا الجزء المتعلق بالتجارة الإلكترونية حيث قرروا:

- توفير البيئة المناسبة لنشر التجارة الإلكترونية بإصدار السياسات والتشريعات اللازمة وتعزيز الآليات الإقليمية لزيادة التبادل التجاري إلكترونيا بين البلدان العربية، وإزالة العوائق التي تعوق تدفق التعاملات التجارية.
- إقامة مؤسسات إقليمية مخولة بسلطة توثيق التوقيع الإلكتروني كأساس للتجارة الإلكترونية.
- توازن العمل في نشر التجارة الإلكترونية مع تحسين خدمات النقل والشحن وخلافه لتسهيل حركة البضائع ما بين البلدان العربية.
- تبني تشريعات موحدة لحماية حقوق المستهلكين والمنتجين وإرساء آليات فض المنازعات.

إعلان القاهرة، الوثيقة العربية، نحو مجتمع معلومات عربي، خطة العمل المشترك، القاهرة في 18 يونيو "حزيران" 2003.

(1) صادرة بالوثيقة رقم A،03/GENEVA/DOC/5،WSIS والتي جاء فيها أن:
خطة العمل هذه تترجم الرؤية المشتركة والمبادئ التوجيهية الواردة في إعلان المبادئ إلى خطط عمل ملموسة للتقدم في إحراز الأهداف الإنمائية المتفق عليها دوليا، بما فيها الأهداف الواردة في إعلان الألفية، وتوافق آراء مونتيري، وإعلان جوهانسبرج وخطة التنفيذ، من خلال النهوض باستعمال المنتجات والشبكات والخدمات والتطبيقات القائمة على تكنولوجيا المعلومات والاتصالات، ومساعدة البلدان على تجاوز الفجوة الرقمية، وسيقوم مجتمع المعلومات المتوخى في إعلان المبادئ بتعاون وتضامن بين الحكومات وجميع أصحاب المصلحة الآخرين.

أ) تشجيع الحكومات والمنظمات الدولية والقطاع الخاص على تعزيز فوائد التجارة الدولية، واستعمال الأعمال التجارية الإلكترونية، والنهوض باستعمال نماذج الأعمال التجارية الإلكترونية في البلدان النامية والبلدان التي تمر اقتصادياتها بمرحلة تحول.

ب) ينبغي للحكومات أن تسعى إلى حفز استثمارات القطاع الخاص، وتشجيع التطبيقات الجديدة، وتطوير المحتوى، والشراكات بين القطاعين العام والخاص، وذلك من خلال اعتناق بيئة تمكينية، واستنادًا إلى إتاحة النفاذ إلى شبكة الإنترنت على نطاق واسع.

ج) ينبغي لسياسات الحكومات أن تؤيد تقديم المساعدة إلى المشروعات الصغيرة والمتوسطة والمتناهية الصغر وتنميتها في صناعة تكنولوجيا المعلومات والاتصالات، علاوة على دخولها إلى الأعمال التجارية الإلكترونية، من أجل حفز النمو الاقتصادي وخلق الوظائف كعنصر في إستراتيجية للحد من الفقر من خلال خلق الثروات.[1]

الفرع الثاني

المرحلة الثانية تونس 2005

التزم المجتمعون في مرحلة تونس ببناء مجتمع معلومات ذي توجه تنموي، يقوم على أساس أغراض ومبادئ ميثاق الأمم المتحدة والقانون الدولي والتعددية[2]، والاحترام الكامل والالتزام بالإعلان العالمي لحقوق

(1) www.itu.int/dms_pub/itu.s/md/03/wsis/doc/S03،WSIS، DOC،0005!!MSW،A.

(2) تمت المرحلة الثانية في تونس في الفترة من 16-18 نوفمبر 2005، وتعد هذه القمة العالمية لمجتمع المعلومات تأكيدا جديدا ودعما لإعلان المبادئ وخطة العمل المعتمدين في المرحلة الأولى من القمة العالمية لمجتمع المعلومات في جنيف =

الإنسان، حتى يتسنى للناس في كل مكان إنشاء المعلومات والمعارف والنفاذ إليها، واستعمالها والمشاركة فيها وتبادلها، كي يحققوا إمكانياتهم بالكامل ويبلغوا الأهداف والمقاصد الإنمائية المتفق عليها دوليًا، بما في ذلك الأهداف الآتية:

1) تحقيق الطابع العالمي لجميع حقوق الإنسان، وترابطها بما فيها الحق في التنمية المستدامة وفقًا لإعلان فيينا، واحترام سيادة القانون في الأمور الدولية والوطنية.

2) إذكاء الوعي بتكنولوجيا المعلومات والاتصالات وما تحمله من فوائد للإنسانية، وتحقيق الأهداف والغايات الإنمائية المتفق عليها دوليًا، والتدريب على إدارة شبكة الإنترنت والمسائل المتصلة بها.

3) الاستفادة من الفرص التي يمكن أن تنشأ عن تكنولوجيا المعلومات والاتصالات لكل من الحكومات، وكذلك القطاع الخاص والمجتمع المدني والأمم المتحدة والمنظمات الدولية الأخرى، والنفاذ إلى البنية التحتية للمعلومات والاتصالات وتكنولوجياتها، وكذلك إلى المعلومات والمعارف، وبناء الطاقات وزيادة الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات.

4) المشاركة في المعرفة والنفاذ إلى المعلومات وإنشائها لتعزيز التنمية الاقتصادية والاجتماعية والثقافية، وإزالة الحواجز أمام النفاذ إلى المعلومات للجميع بشكل شامل ومنصف ويسير التكلفة.

5) تمكين القدر الأكبر من السكان من اللحاق بركب المعرفة الإنسانية وتقاسمها، وتوسيع قاعدتها وزيادة نموها وتطبيقاتها في التعليم والصحة والعلوم، وتنطوي تكنولوجيا المعلومات والاتصالات على

= في ديسمبر 2003.

إمكانيات هائلة وإدخال طرق جديدة من التعليم ودعم محو الأمية والتعليم الأولي للجميع.

6) تبني المؤسسات لتكنولوجيا المعلومات والاتصالات له دور أساسي في تحقيق النمو الاقتصادي، وزيادة الإنتاجية الناتجة عن استثمارات وزيادة التجارة وتحسين فرص العمل، بالمشاركة بينها وبين الحكومات والقطاع الخاص لتعزيز قدراتها، مع العمل على وضع السياسات اللازمة والأطر القانونية والتنظيمية الضرورية لرعاية إقامة المشروعات، وخاصة للمؤسسات المتوسطة الحجم والصغيرة والمتناهية الصغر.

7) بناء البنية التحتية لتكنولوجيا المعلومات والاتصالات، والتأكيد على تنمية القدرات البشرية، وعلى تهيئة تطبيقات تكنولوجيا المعلومات والاتصالات، ومحتوى رقمي باللغات المحلية للوصول إلى نهج شامل لبناء مجتمع معلومات عالمي.

8) النفاذ الشامل دون تمييز إلى تكنولوجيا المعلومات والاتصالات لجميع البلدان، مع ضرورة مراعاة مستوى التنمية الاجتماعية والاقتصادية لكل بلد، واحترام نواحي مجتمع المعلومات ذات التوجه التنموي، وسد الفجوة الرقمية، لكي يمكن بلوغ الأهداف والغايات الإنمائية المتفق عليها دوليًا، وتعزيز جهود التعاون الدولي في بناء مجتمع المعلومات، مع إقامة أنظمة عامة للمعلومات بشأن القوانين والقواعد، لاستفادة الجميع من المزايا التي تتيحها تكنولوجيا المعلومات والاتصالات للتنمية.

9) تطوير مجتمع المعلومات لتحقيق الاحتياجات الخاصة لشعوب البلدان النامية والبلدان التي تمر اقتصادياتها بمرحلة تحول، والبلدان الأقل

نموًا، والبلدان الفقيرة المثقلة بالديون، والأراضي الواقعة تحت الاحتلال، مع تشجيع جميع أصحاب المصلحة على مساندة مشاركة المرأة في عمليات صنع القرار، والمساهمة في تشكيل جميع نواحي مجتمع المعلومات على الصعيد الدولي والإقليمي والوطني.

10) تكنولوجيا المعلومات والاتصالات تشمل الحاضر (وهم الشباب) والمستقبل (وهم الأطفال) ولأجل ذلك يجب تعلم برامج التنمية المبتكرة التي تقوم على أساس تكنولوجيا المعلومات والاتصالات، والاندماج في عمليات الإستراتيجيات الإلكترونية، والتغلب على الفجوة الرقمية وتحقيق أهداف وغايات التنمية المتفق عليها دوليًا.

11) تطوير نظام تجارة عالمي متعدد الأطراف يقوم على الشراكة بين الحكومات والقطاع الخاص والمجتمع المدني والأوساط العلمية والأكاديمية والمستخدمين لمختلف التكنولوجيات، على أساس حكم القانون والانفتاح وعدم التمييز والإنصاف وحفز التنمية على نطاق العالم، مما يؤدي إلى شمول مجتمع المعلومات لجميع الشعوب، من خلال تطوير واستعمال اللغات المحلية في تكنولوجيا المعلومات والاتصالات.

المطلب الثالث

الشراكة المجتمعية وتنظيم التجارة الإلكترونية

يأتي مجتمع المعلومات بعد مراحل متعددة مر بها التاريخ الإنساني، وتميزت كل مرحلة بخصائص ومميزات، حيث شهدت الإنسانية من قبل تكنولوجيا الصيد، ثم تكنولوجيا الزراعة، وبعدها تكنولوجيا المعلومات التي رسمت الملامح الأولى لمجتمع المعلومات، هذا الأخير تميز بالتركيز على

العمليات التي تعالج فيها المعلومات، والمادة الخام الأساسية به هي المعلومة، التي يتم استثمارها بحيث تولد المعرفة، معرفة جديدة، وهذا عكس المواد الأساسية في المجتمعات الأخرى حيث تنضب بسبب الاستهلاك، أما في مجتمع المعلومات فالمعلومات تولد معلومات، مما يجعل مصادر المجتمع المعلوماتي متجددة ولا تنضب، الأمر الذي يفسر أهمية المعلومات، ومكانتها كأهم مادة أولية على الإطلاق، وهو ما يجعل المجتمع الجديد يعتمد في تطوره بصفة أساسية على هذا المورد، وشبكات الاتصال والحواسيب، ويتميز بوجود سلع وخدمات معلوماتية لم تكن موجودة من قبل، إلى جانب اعتماده بصفة أساسية على التكنولوجيا "الفكرية" أي تعظيم شأن الفكر والعقل الإنساني بالحواسيب والاتصال والذكاء الاصطناعي ونظم الخبرة.[1]

وتعد مشاركة المجتمع المدني أمرًا لا غنى عنه من أجل إقامة مجتمع منصف للمعلومات، يقوم على التنمية الاقتصادية والاجتماعية المستدامة،

(1) في مجتمع المعلومات يشكل قطاع المعلومات المصدر الأساسي للدخل القومي والعمل والتحول البنائي، ففي الولايات المتحدة ينتج قطاع المعلومات حوالي نصف الدخل القومي وفرص العمل، وتظهر اقتصاديات الدول المتقدمة في أوروبا أن حوالي 40 بالمائة من دخلها القومي قد انبثق من أنشطة المعلومات في منتصف السبعينيات، ورغم تعدد المفاهيم حول مجتمع المعلومات إلا أنه يمكن استشفاف أن مجتمع المعلومات يرتكز أساسا على إنتاج المعلومة، والحصول عليها، واستغلالها في خدمة أهداف التنمية والتطوير، من خلال وضع آلياتها وإدارة انسيابها بواسطة بنية تحتية للمعلومات وشبكات الاتصال، ويمكن القول بأن أهم عنصر لقيام مجتمع معلومات مبني على قيمة المعرفة وإتاحة عادلة للوصول إلى المعلومات هو تنمية الإدراك البشري ومهارة استخدام تكنولوجيا المعلومات.
http://ar.wikipedia.org/wiki/

وتعد هذه المشاركة للمجتمع المدني أمرًا حيويًا يحظى مجتمع المعلومات من خلاله بالقبول الاجتماعي، ومن شأنها المساعدة على تقوية عنصر القيمة داخل مثلث: "التنظيم، والأسواق، والقيم"، والذي عجل بإقامة مجتمع المعلومات ونموه.

كما تعد مشاركة القطاع الخاص أمرًا حيويًا في مجتمع المعلومات، من أجل ضمان التنمية السليمة والمستدامة للبني التحتية والمحتوى والتطبيقات الميسورة لهذا المجتمع المعلوماتي، ويمكن إشراك القطاع الخاص في صورة اتفاقيات عملية للشراكة لتحقيق التطبيقات المبتكرة، مثل مبادرات الحكومات الإلكترونية، ويتخطى دور القطاع الخاص دور السوق، فيمكنه أن يلعب دورًا داخل سياق سياسي واجتماعي أوسع من خلال مساعدة البلدان -على سبيل المثال- على استقدام تكنولوجيا المعلومات والاتصال، وإقامة الأسواق الخاصة بها، وتطوير قدرة الموارد البشرية اللازمة لتقليل الهوة الرقمية.[1]

والشراكة المجتمعية تعني إشراك شرائح المجتمع المحلي في آلية أو تنظيم مؤسسي محلي لا مركزي، يشارك في مختلف مجالات التنمية الشاملة المرتبطة بالعمل المحلي في الدولة، سواء أكانت خدمية أو ثقافية أو اقتصادية أو اجتماعية، على شكل مجموعات أو جماعات في مؤسسات غير ربحية، منتخبة أو معينة، تتلقى دعمًا رسميًا وشعبيًا وتفويضًا في مؤسساتها ومشروعاتها التنموية، وتخضع لإشراف إدارة عليا، وتكون جسرًا بين أهالي المنطقة - بمختلف مسمياتها وحدودها - وبين الأجهزة التشريعية والتنفيذية والمؤسسات المجتمعية محليًا وإقليميًا وعالميًا ضمن سياسة الدولة، بحيث تحقق مبادئ وأسس الشراكة في العمل المحلي والخدمات المرتبطة

(1) http://www.un.org/arabic/conferences/wsis/faq3.htm

بـه، وتمـارس في مزاولـة مهامهـا واختصاصـها ومراقبتهـا وتقويمهـا وتحفيزهـا مـن أجـل تنفيـذ المشروعات وإدارتها وصيانتها واستمراريتها سياسة واضحة تعتمد المشورة والخبرة والعدالة والشفافية.[1]

وسنتحدث في هذا المطلب حول هذه الشراكة المجتمعية، ودورها في مجتمع المعلوماتية، ومتطلبات هذه الشراكة في فرع أول، ثم نتحدث عن المجتمع المدني، ودوره في ثورة المعلومات أو الثورة الرقمية في فرع ثان.

(1) كما قرر ممثلو الحكومات العربية في المؤتمر العربي رفيع المستوى بمدينة القاهرة المنعقد للتحضير لمؤتمر القمة العالمية لمجتمع المعلومات السابق الإشارة إليه بخصوص الشراكة المجتمعية ما يلي:

- تشجيع أنماط الشراكة المختلفة بين مؤسسات القطاع الخاص بعضها البعض، وبينها وبين القطاع العام، وبينها وبين الشركات متعددة الجنسيات، للإسراع بعمليات توطين تكنولوجيا المعلومات والاتصالات في المؤسسات العربية.
- إتاحة الفرص لمؤسسات المجتمع المدني للمساهمة في الترويج لمجتمع المعلومات وتنمية الطلب المحلى وتقوية التضامن الرقمي.
- طرح بدائل عديدة ومبتكرة ونماذج متنوعة للأعمال الإلكترونية مشاركة بين الحكومة والقطاع الخاص.
- تبسيط الإجراءات، وزيادة عناصر الجذب للاستثمارات الإقليمية والأجنبية للإسراع في إرساء البنى التحتية، وإقامة صناعة المحتوى العربية.
- توفير المعلومات اللازمة للاستثمار وتحديثها دوريًا، وإتاحتها للمجتمعين الإقليمي والدولي، مع حث المستثمرين وجهات الدعم على الاستعانة بشركاء محليين.

إعلان القاهرة، الوثيقة العربية، نحو مجتمع معلومات عربي، خطة العمل المشترك، القاهرة في 18 يونيو "حزيران" 2003.

الفرع الأول

دور الشراكة المجتمعية

تتنوع الشراكات في مجالات العمل المجتمعي من الشراكة البسيطة بين الأفراد إلى الشراكة الكبيرة بين المؤسسات والمنظمات محليًا أو إقليميًا أو عالميًا تحت عدة مسميات؛ والمجالس البلدية واحدة من هذه التنظيمات، كما أن لمؤسسات المجتمع المدني دورًا كبيرًا في تطوير وتفعيل العمل المجتمعي، لتحقيق شراكة أفضل لطبقات المجتمع وشرائحه لتكون شريكًا أساسيًا في ميادين التنمية الاقتصادية والاجتماعية والثقافية.

وتضطلع الشراكة المجتمعية في العمل المجتمعي بدور محوري أساسي وفاعل في بناء الدولة ومؤسساتها ثقافيًا واجتماعيًا واقتصاديًا وسياسيًا، في عالم يمتاز بالتطور التكنولوجي والإعلامي والتكامل الاقتصادي والاجتماعي، والانفتاح السياسي، والسعي نحو ديمقراطية الأنظمة والقوانين والخدمات، بحيث يكون كل عنصر في الدولة لا غنى عنه في الحقوق المعطاة له أو في الواجبات المطلوبة منه، أو الأدوار الملقاة عليه، وكل فكرة رائدة أو تجربة ناجحة أو ممارسة موفقة لها مجال في التخطيط والتطبيق والتقويم والاستفادة يمكن استثمارها في التنمية والتطوير، في جو من التقدير والتحفيز لنيل ثمرة يتقاسمها الجميع بعدالة.

ولقد سهل التقدم في وسائل الاتصال نقل الأفكار وتبادلها وانتقال الثقافات والتأثر بها، مما ساهم في تغيير أساليب الحياة والتغير والتغيير في الاتجاهات، والارتقاء في مستوى طموح الأفراد وتطلعاتهم، مما خلق لهم نموًا عقليًا ونماءً في التفكير ساهم في رغبتهم في المشاركة في إدارة شئونهم المحلية واستثمار إمكانياتهم في التنمية للحصول على مكاسبها،

خاصة في المجتمعات المتقدمة إعلاميًا وعلميًا وتقنيًا، وجرت وراءها المجتمعات النامية تأثرًا بما تحقق لشعوبها (أي شعوب الدول المتقدمة) من سبق وعراقة ومكاسب سياسية واجتماعية.

ولضمان تحقيق شراكة فاعلة لابد من بناء إستراتيجية تتناول مؤسساتها وفلسفتها القائمة على الجانب المعرفي، وعلى المهارة والتغيير القيمي، وتغيير الاتجاهات، والدعم والتأييد، واستثمار الوقت والجهد، والعمل بآليات التنسيق والتكافل، وإصدار أنظمة ولوائح تنظيمية توضح مفهوم الشراكة وحدودها وأنظمتها وشروط تشكيلها، وحقوق وواجبات ومسئوليات أعضائها، وآلية إشهارها والوصاية عليها، ويتطلب ذلك وضع هيكل لبنائها، وقواعد وأنظمة معلوماتية وتشريعية ومالية، وتحديد جهات توجيهية ورقابية، والاتفاق على اختصاصات واضحة، وتوفير تجهيزات كافية، والاستعانة بخبرات واستشارات مناسبة، وتقديم مساعدات إدارية ومالية وفنية وتقنية لها، ومن بينها توفير مقار مجهزة لعمل الجماعات المتشاركة، وتوعية وتثقيف وتدريب المنتسبين إليها، وتقديم تسهيلات لعملها، وتبسيط إجراءات معاملاتها، وتحفيزها وتشجيعها على المشاركة الفاعلة.

الفرع الثاني

دور المجتمع المدني

تطور مفهوم المجتمع المدني من المفهوم الشخصي القديم، حيث كان يعني مجموع المواطنين الذين يرتبطون برباط المواطنة، وذلك في بداية نشأته في المجتمع اليوناني القديم، حيث وجد تاريخيًا بشكل بدائي منذ أرسطو[1]، أما اليوم فقد تحول هذا المفهوم الشخصي إلى مفهوم موضوعي،

(1) د. مصطفى المصمودي، المجتمع المدني العربي في زمن الثورة الرقمية، =

فأصبح مفهومه المعاصر هو مجموع القيم المشتركة، وهو الذي يشكل رأس المال الاجتماعي.

وقد أخذ الإتجاه الحديث بالمفهوم الشخصي وبالمفهوم الموضوعي، فأصبح المجتمع المدني يتألف من كل الأفراد والمنظمات ممن يبذلون جهدهم بدون هدف الربح، ويناضلون من أجل احترام القيم العالمية وحقوق الإنسان والديمقراطية والقانون الدولي، ويعملون بالاعتماد على الوسائل السلمية وباستقلال عن المصالح التجارية والسلطة العمومية والأحزاب السياسية والبرامج الدينية، ويسعون لتهيئة الرأي العام، وتعميق الوعي الجماعي بالقضايا العامة والتضامن الاجتماعي، والمساواة بين الذكور والإناث، والتعددية الثقافية، وسبل تحسين نوعية الحياة ونظافة المحيط، وحماية الطبيعة، ومشاركة المواطنين في الحياة السياسية.

وقد حددت لجنة الخبراء التابعة لمنظمة الأمم المتحدة مستقبل العلاقة بين التنظيم الأممي والمجتمع المدني، وعرفت المجتمع المدني بأنه النشاط المجتمعي للمواطنين خارج دوائر العلاقات الضيقة كالعائلة والصداقة والزمالة، بحيث يتمكن الإنسان من الدفاع عن مصالحه وأفكاره ومبادئه، مع استثناء كل نشاط تجاري من شأنه تحقيق الربح أو أي نشاط سياسي أو ديني.[1]

وتعتمد منظمة الأمم المتحدة عبارة "المنظمات غير الحكومية" للإشارة إلى كل المنشآت التي لا تنتمي إلى الهيئات الحكومية والمنظمات الدولية.

ويمكن أن ينتسب كذلك إلى المجتمع المدني كل فرد يمارس نشاطه

= دار البستان للنشر، تونس، نوفمبر 2005، ص 24.

(1) د. مصطفى المصمودي، المجتمع المدني العربي في زمن الثورة الرقمية، المرجع السابق، ص 24.

المهني في الإطار التربوي والعلمي والثقافي، وبذلك تتجاوز تركيبة المجتمع المدني الجمعيات والتشكيلات الاجتماعية لتشمل كل الأطراف الفاعلة خارج النطاق الحكومي والقطاع التجاري، والتي تسخر جهدها لدعم المبادرات المبنية على التطوع والتآزر والتضامن، ولذلك فقد ميز التشريع في كثير من البلدان بين قوانين الأحزاب وقوانين الجمعيات؛ حتى لا تختلط الأوراق فتصبح الأحزاب نوادي مهنية والجمعيات أحزابًا سياسية.

وبما أن الحياة السياسية تدعو المواطنين أفرادًا وجماعات إلى الاهتمام بكل القضايا العامة، فقد حاول بعض المنظرين التوفيق بين الاعتبارين الشخصي والموضوعي ووضع الحدود الفاصلة بينهما.

وفي هذا السياق يؤكد التعريف الذي طرحته الأمم المتحدة على دور هذا المجتمع في تحسين نوعية الحياة للفئات المهمشة، ودعم تلك الفئات، والإسهام في التحول الديمقراطي.[1]

---

(1) أطلقت مكتبة الإسكندرية مبادرة السوق العربي للمعلومات (Arab Info Mall) بهدف إتاحة الوصول إلى أنشطة المنظمات غير الحكومية ومنظمات المجتمع المدني, وهي من المبادرات الرائدة في هذا المجال، وقد نصت التوصيات الصادرة عن مؤتمر الإصلاح العربي الأول الذي عقد بمكتبة الإسكندرية في مايو 2004 على أهمية إنشاء السوق العربي للمعلومات ليكون بمثابة نقطة التقاء للمجتمع المدني العربي ولإثراء معرفة منظمات المجتمع المدني بالمنظمات الأخرى وأنشطتها، ويشبه مجتمع المعلومات العربي الذي يجري إنشاؤه مركزًا أو سوقًا تجتمع به المنظمات غير الحكومية ومنظمات المجتمع المدني في بوابة إلكترونية تعرض محتواها بثلاث لغات هي العربية والإنجليزية والفرنسية، ويُخصص لكل منظمة من المنظمات المشاركة مقر يمثلها داخل السوق، وتمثل هذه المبادرة نقطة وصول على شبكة الإنترنت تتيح للمنظمات غير الحكومية المصرية والعربية إمكانية تقديم أنشطتها والتعرف على الأنشطة التي يقوم بها الآخرون، وهو ما يوفر الفرصة أمام هذه المنظمات للمشاركة النشطة والفعالة في أنشطة الإصلاح =

ويتوجه العالم بكل قوة نحو التوسع في دور مؤسسات المجتمع المدني إيمانًا منه بأن التنمية الشاملة لا تتحقق إلا بمشاركته وبمبادراته[1]، غير أن دور هذه المؤسسات قد انحصر في بعض البلدان العربية في دوائر محدودة من العمل الاجتماعي[2]، وعلى كل فقد برهنت التطورات المعاصرة على أهمية المنظمات الأهلية.

هذا وقد حاولت المؤتمرات التحضيرية لقمة مجتمع المعلومات إشراك منظمات المجتمع المدني إلى جانب الحكومات والقطاع الخاص في المفاوضات، وهو تقليد جديد يتبع لأول مرة في قمة دولية، وتم بالفعل إشراك ممثلي المجتمع المدني في النقاش، بحيث كان بإمكانهم تقديم الأفكار ومناقشتها على أن يتخذ ممثلو الحكومات قرار القبول أو الرفض،

= المنشورة، ويمهد الطريق لتكوين شراكات أكثر قوة ونجاحا، وينظر إلى مبادرة السوق العربي للمعلومات كأداة لمنتدى الإصلاح العربي يمكن من خلالها تقديم مزيد من الدعم لقضايا الديمقراطية والحرية والسلام عن طريق تشجيع جهود المجتمع المدني التي تسعى لتوطيد مفاهيم الإصلاح والحوار بالمنطقة، وقد روعي في تصميم موقع السوق العربي للمعلومات توفير آلية لامركزية يمكن من خلالها لكل كيان من الكيانات المشاركة في السوق أن تقوم بالإضافة إلى البيانات التي تُعرض في مقرها، وتحديثها بما يضمن حداثة وفاعلية المعلومات المقدمة، وتلقي النسخة التجريبية www.arabinfomall.org التي تم إطلاقها في أبريل 2005 الضوء على أنشطة ومشروعات المنظمات غير الحكومية ومنظمات المجتمع المدني، إلى جانب بيانات الاتصال الخاصة بهذه المنظمات من خلال نشرة أخبار. http://www.egyptatwsis.com.eg/ar/Partners.asp

(1) د. أماني قنديل، ندوة (مستقبل مؤسسات المجتمع المدني في دول مجلس التعاون الخليجي) 3، 4 أبريل 2000، مركز جامعة الخليج والجزيرة العربية (جامعة الكويت).

(2) د. ميمونة الصباح في كلمتها الافتتاحية للندوة المذكورة.

ولكن بعد تعثر المفاوضات أعربت منظمات المجتمع المدني عن أنها لا ترغب في الموافقة على وثيقة يدور حولها جدل كبير، وهذا ما عبر عنه ممثلو المجتمع المدني، فقد قررت منظمات المجتمع المدني تقديم وثيقة سياسية منفصلة عن وثيقتي القمة تعرض فيها تصوراتها لمجتمع المعلومات، وكانت تلك المنظمات قد أوضحت في بيان مشترك أن الأعمال التحضيرية للقمة "فشلت لحد الآن في الاتفاق حول النقطتين الأكثر أهمية: التضامن بين الشمال والجنوب، والالتزام بحقوق الإنسان".[1]

وفي قمة تونس طالب ممثلو المجتمع المدني في القمة الحكومات برفع الرقابة المفروضة على شبكة الإنترنت، وإطلاق سراح السجناء السياسيين وسجناء الرأي، أما البلدان الإفريقية فقد دعا ممثلوها إلى الحد من التمييز العرقي ضد القارة، وتقليص الفجوة الرقمية بين بلدان الشمال والجنوب.[2]

وحتى يشمل التطور كافة القطاعات وجميع الفئات أوصت بيوت الخبرة بالتعاون بين كل القطاعات المعنية والمنظمات الدولية المختصة مثل منظمة التجارة العالمية والاتحاد الدولي للاتصالات واليونسكو لإعداد المناخ الدولي الملائم، وجاءت اللوائح الأولى الصادرة عن قمة المعلومات على ضرورة العناية المطلقة بأهداف الألفية للتنمية من خلال النشاط الرقمي، وحتمية هذه الشراكة بين كافة الأطراف الذين وصفتهم بأصحاب المصلحة لبناء مجتمع

(1) http://www.swissinfo.org/ara/news/science_technology.html?siteSect=511&sid=4458716&cKey=1070636924000&ty=st

(2) أصيبت منظمات المجتمع المدني بخيبة أمل على إثر قرار الإبقاء على سيطرة الولايات المتحدة على شبكة الإنترنت، والذي جاء في اتفاقية تسوية عشية قمة مجتمع المعلومات الثانية في تونس، ووفق الاتفاقية فإن منظمة الآيكان الأمريكية والتي مقرها كاليفورنيا والتي لها التحكم التكنولوجي في شبكة الإنترنت سوف تبقى متحكمة في الشبكة الدولية.

http://www.ipsterraviva.net/TV/tunis/printArabic.asp?idnews=21

المعلومات، وفي مقدمتهم المنظمات غير الحكومية.

وقد أوضحت إحدى الدراسات المتعمقة التي أجراها برنامج الأمم المتحدة للتنمية في سنة 2000 أن مساهمة قطاع المجتمع المدني في الناتج الوطني تتراوح بين 8 و14 في المائة بالنسبة إلى 13 بلدًا مصنعًا، وهذه النسبة بعيدة المنال في الوقت الحاضر لأغلب البلدان العربية، وقد تتجاوز في أحسن الحالات مقدار 3 بالمائة، ولذلك فإنه من الصالح التحرك من أجل إدراج برامج النشاط الأهلي في المخططات الوطنية.[1]



(1) د. مصطفى المصمودي، المجتمع المدني العربي في زمن الثورة الرقمية، مرجع سابق، ص 39.

المبحث الثالث

التجارة الإلكترونية في التشريعات الوطنية

تكمن المشكلة الرئيسية في عدم قدرة القانون على مسايرة التكنولوجيا الجديدة، حيث إن هناك فراغًا تشريعيًا واسعًا في مجال التجارة الإلكترونية، مما أدى إلى العديد من المشكلات التي تفتقر إلى وجود حل قانوني، الأمر الذي يؤدي إلى وجود عقبات تعيق انطلاق المعاملات الإلكترونية البينية من جهة، والمعاملات الدولية من جهة ثانية، وقد تنبه المشرع في العديد من الدول العربية والأجنبية إلى أهمية تنظيم التجارة الإلكترونية وحمايتها، لتشمل كل معاملة تجارية تتم عن بعُد باستخدام وسيلة إلكترونية "[1]، وقامت العديد من الدول مثل سنغافورة وأستراليا والمملكة المتحدة وأيرلندا، بإصدار قوانين لتنظيم التجارة الإلكترونية وكذا الحال لدى بعض الدول العربية، والملاحظ على أغلب القوانين المنظمة للتجارة الإلكترونية أنها لم تضمن تعريفًا لماهية التجارة الإلكترونية تاركة هذه المهمة للفقه، وسوف نتناول في هذا المبحث التدابير التشريعية في الدول الأجنبية، ثم التدابير التشريعية المتخذة في الدول العربية في المطلبين التاليين:

المطلب الأول: التجارة الإلكترونية في التشريعات الأجنبية

المطلب الثاني: التجارة الإلكترونية في التشريعات العربية

---

(1) د. خالد حمدي عبد الرحمن، التعبير عن الإرادة في العقد الإلكتروني، دار النهضة العربية، 2007، ص 20.

المطلب الأول

التجارة الإلكترونية في التشريعات الأجنبية

أصدرت بعض الدول الأجنبية قوانين منظمة للتجارة الإلكترونية، وعلى رأسها الولايات المتحدة الأمريكية والتي تعد من أوائل الدول التي سعت وبقوة إلى تنظيم عمل هذه التجارة الإلكترونية، وسوف نتناول بالدراسة بعض القوانين الأمريكية المتعلقة بالتجارة الإلكترونية، ثم نتطرق لبعض الدول الأخرى كالمملكة المتحدة، وكندا، وفرنسا، ولوكسمبورج، وإيطاليا، واليابان، والهند، وماليزيا, وسنغافورا.

أولا: الولايات المتحدة الأمريكية:

تحتل الولايات المتحدة الأمريكية المرتبة الأولى في الاستعداد الإلكتروني, والمرتبة الأولى في التعاملات الإلكترونية, حيث صنفت أولى الدول في الاستعداد الإلكتروني وفقا لآخر الإحصائيات, ويعود ذلك إلى عدة أسباب من أهمها وجود البيئة القانونية المناسبة والتي تمثل الغطاء الشرعي للتعاملات الإلكترونية, والذي أعطاها الثقة والمصداقية, وساهم بشكل مباشر في انتشارها وتسارع نموها وإقبال الأطراف عليها[1].

وأصدرت الحكومة الأمريكية العديد من القوانين في هذا المجال، ومنها قانون جرائم الكمبيوتر الفيدرالي أو القانون الخاص بمكافحة الغش والاستخدام غير القانوني, وقانون الاتصالات في فبراير 1996, وقانون

(1) د. سليمان بن محمد الشدي، الجانب التشريعي والقضائي في دول مجلس التعاون لدول الخليج العربية ودوره في دعم التعاملات والتجارة الإلكترونية، المؤتمر العلمي السنوي السابع عشر المعاملات الإلكترونية (التجارة الإلكترونية - المعاملات الإلكترونية) 19-20/ مايو 2009، تنظيم جامعة الإمارات العربية المتحدة، مركز البحوث والدراسات الإستراتيجية.

خصوصية الاتصالات الصادر عام 1998, وقانون اعتماد التواقيع والسجلات الإلكترونية الصادر في 20 مارس 1997.

كما أصدرت الولايات المتحدة تقريرًا في 1997/7/1 بشأن التجارة الإلكترونية ضمنته مبادئ عامة لإقامة منطقة تجارة حرة على شبكة الإنترنت تشمل العالم كله.

ففي ذلك العام اطلق الرئيس الامريكي خطة العمل الخاصة بالتجارة الالكترونية، وتضمنت الخطة مبادئ رئيسة خمسة هي:- اسناد قيادة التجارة الالكترونية للقطاع الخاص، وتجنب الحكومة وضع القيود أمام الاستثمار والأنشطة الإبداعية في ميدان التجارة الالكترونية، وللحكومة دور في كفالة وحماية الملكية الفكرية والخصوصية وأمن الشبكات والمعلومات والشفافية والسرعة في حل المنازعات، وعلى الحكومة دور في البناء الفاعل للوسائل التقنية ووسائل الاتصال، والانترنت بيئة عالمية وإطارها القانوني يتعين ان يكون عالميا وتحديدا بالنسبة للاختصاص القضائي.

وسندا لهذه المبادئ تضمنت الخطة تسع توصيات رئيسة متصلة بالجوانب القانونية والتنظيمية للتجارة الالكترونية، وتتمثل هذه التوصيات، بعدم فرض اية ضرائب او تعرفة على أنشطة التجارة الالكترونية وإيجاد نظام قانوني مرن للدفع النقدي يراعي سرعة التطور التقني لوسائل الدفع، وتعديل القواعد القانونية التجارية بالنسبة للعقود التجارية والتواقيع الالكترونية وقواعد الدفع والتبادل المالي، حماية الملكية الفكرية وضمان حقوق المعلنين والمستثمرين المعنوية فيما ينشر الكترونيا وبخصوص الحلول التقنية والبرمجيات ذات العلاقة، حماية الخصوصية بحظر جمع البيانات الخاصة إلا وفق القواعد التي تكفل حماية أصحابها وصحة البيانات والحق في تعديلها ومعرفة أوجه استخدامها ومعالجتها، وحماية أمن

المعلومات وأمن الشبكات وخلق معايير تشفير مقبولة، وإزالة كافة القيود أمام صناعة التقنية والاتصالات، وتشجيع التنظيم الخاص من قبل القطاعات الصناعية التقنية بشأن القيود المفروضة على المحتوى المنشور ضمن القطاعات العاملة على الانترنت، وإيجاد معايير تقنية لأعمال الانترنت مستندة للسوق وليس الى معايير حكومية مفروضة.[1]

وتسترشد الحكومة الأمريكية بهذه المبادئ في دعم تطور التجارة الإلكترونية، كما تقدم هذه المبادئ توصيات بشأن المجالات الرئيسية لهذه التجارة، خصوصًا في مجال المحافظة على شبكة الإنترنت باعتبارها وسيلة التعامل بحيث لا تكبلها قيود تنظيمية، بل يترك فيها المجال للمنافسة واختيارات الموردين والمستوردين لتحديد شكل وطبيعة السوق، وأهم هذه المبادئ, كما رأينا, هي تولي القطاع الخاص الدور القيادي في تطوير شبكة الإنترنت وتشجيع التنظيم الذاتي، وتتجنب الحكومات فرض قيود غير ضرورية على التجارة الإلكترونية، بحيث يتم تنظيمها باتفاقيات بين الأطراف صاحبة المصلحة، كما أنه يجب أن يكون دور الحكومة إذا دعت الحاجة إلى تدخلها هو تأمين المنافسة، وحماية الملكية الفكرية، وحماية الخصوصية، ومنع الغش، وتشجيع الشفافية، وتسهيل حل المنازعات.

كما يلزم الحكومة أن تدرك خصائص شبكة الإنترنت، وأن تدرك أن نجاحها يعزى إلى طبيعتها غير المركزية وتجاوزها الحدود الجغرافية، لذلك فإنه يلزم مراجعة القوانين المعمول بها حاليًا في مجال الاتصالات السلكية واللاسلكية والراديو والتلفزيون، والتي قد تعيق التجارة الإلكترونية، كما يجب التعامل مع التجارة الإلكترونية عن طريق شبكة الإنترنت على أساس

(1) يونس عرب - التجارة الالكترونية - بحث منشور على شبكة الانترنت - ص31 - على الموقع:- doc.abhatoo.net.ma/IMG/doc/dro8.doc

عالمي؛ لذا فإنه يلزم أن تكون القوانين المنظمة لها آخذة في اعتبارها ذلك.

ولقد أصدرت العديد من الولايات الأمريكية قوانين متعلقة بالتجارة الإلكترونية, وتعد ولاية كاليفورنيا أول ولاية تصدر قانونا للتجارة الالكترونية وذلك بإصدار قانون المعاملات الالكترونية الموحد في 16 سبتمبر 1999, والذي دخل حيز النفاذ في أول يناير 2000, كما أصدرت ولاية نورث كالورينا أيضا قانون المعاملات الالكترونية الموحد, والذي دخل حيز النفاذ في أول أكتوبر 2000, ثم توالت إصدار بعض الولايات الأخرى لقوانين مماثلة وموحدة للمعاملات الالكترونية.

وعلى المستوى الاتحادي صدر القانون الموحد للمعاملات الإلكترونية (UETA)[1] في يونيه سنة 2000 باقتراح من المؤتمر الوطني للمفوضين لقوانين الولايات الموحدة.

وينظم هذا القانون العقود الإلكترونية ويدعم تنفيذها، ويمنح التوقيعات الإلكترونية والرقمية نفس القوة القانونية الممنوحة للتوقيعات الخطية التقليدية، ويستند القانون الأمريكي في ذلك على قاعدة التكافؤ المستمدة من مبدأ النظير الوظيفي المنصوص عليه في قانون (الأونسيترال) النموذجي بشأن التجارة الإلكترونية 1996.[2]

ومع ذلك لم يضع المشرع الأمريكي تعريفًا للتجارة الإلكترونية حين أصدر قانون المعاملات التجارية الإلكترونية، إلا أنه بين في الفقرة الثانية من المادة الثانية ماهية الأعمال التجارية الإلكترونية.

وقد سبق أن أصدر المشرع الأمريكي القانون التجاري

(1) The Uniform Electronic Transactions Act.

(2) John Bagby ,E‹Commerce law (Issues for Business) Thomson‹ South‹ Western west London , 2003, p 421.

الموحد[1] Uniform Commercial Code (UCC) والذي نص في المادة الرابعة منه على تحويل الأموال إلكترونيًا Electronic Fund Transfer (EFT) سواء بين البنوك أو في سداد المدفوعات والالتزامات بطريقة إلكترونية[2] وذلك باستخدام نظام المقاصة الإلكترونية أو بطاقات الائتمان أو ماكينات الصرف الآلي - ومنها البطاقة الذكية - أو النقود الإلكترونية فيما بين البنوك والأشخاص ووحدات الأعمال.[3]

ثانيًا: المملكة المتحدة:

ينص قانون الاتصالات الإلكترونية لعام 2000 على أحكام تتعلق بتسهيل التجارة الإلكترونية وتخزين المعلومات، وذلك من ضمن عدة موضوعات، فوفقا للمادة (7) من هذا القانون تعترف المملكة المتحدة بالقوة القانونية للتوقيع الإلكتروني، والمصادقة عليه، والقبول بهذا التوقيع للإقرار بصحة المستند الموقع.

وفي المملكة المتحدة يوجد أحد القوانين المطبقة والمرتبطة بالتوقيع الإلكتروني هو قانون التعاملات الإلكترونية الموحد(Uniform Electronic Transactions ACT (UETA، والذي ينحصر مجال

(1) تجدر الإشارة إلى أنه يجب التفرقة بين القانون الموحد والقانون الفيدرالي في النظام القانوني الأمريكي على النحو التالي:

- القانون الموحد: يتناول موضوعات هي بالأصل من اختصاص الولايات؛ لذلك فإن القانون الموحد هو عبارة عن نموذج قانون أو قانون نموذجي، ويكون للولايات أن تأخذ به أو ترفضه.
- القانون الفيدرالي: يسري وبشكل ملزم على جميع الولايات.

(2) Thomas C.Baxter,Jr _ Sephanie A.Heller ,The ABCs of the UCC , Article 4A: Fund Transfer , by the American Bar Association 1997 p3.

(3) د. خالد ممدوح، إبرام العقد الإلكتروني، مرجع سابق، ص 27.

تطبيقه في المعاملات التي تتعلق بـالأعمال والتجـارة والمسـتهلك والأمـور الحكوميـة، كـما يـنظم قانون التوقيع الإلكـتروني في التجـارة الوطنيـة والعالميـة Electronic Signature in Global and National Commerce ACT E-Sign نشاط هيئات المصادقة، ويضع شروطًا لتطبيـق عملي للتوقيع الإلكتروني، ويؤخذ على هذا القانون أنه لا يتوافـق مـع توصـيات منظمـة التجـارة العالمية وقانون الأونيسـترال وغيرهـا مـن المـنظمات المـؤثرة، كـما أن أنظمـة التوقيـع الإلكـتروني المفصلة فيه غير متوافقة مع المعايير الدولية، وهناك مطالبات بتعديل القانون.

ثالثًا: كندا:

أصدر المشرع الكندي قانون التجارة الإلكترونية الموحد عام 1999,[1] واكتفى بتعريف تعبير "إلكترونيًا" باعتبار أن التجارة نشاط اقتصادي معروف ولها قواعد متفق عليها، ويعني "إلكترونيًا" عملية إنشاء أو تسجيل أو نقل أو تخـزين في صـيغة رقميـة أو أي صـيغة أخـرى غـير ملموسـة، بواسطة وسائل إلكترونية أو بأي وسائل أخرى مشابهة، لديها القدرة على الإنشاء أو التسـجيل أو النقل أو التخزين إلكترونيًا".[2]

(1) وهو يتكون من خمـس وعشرـين مـادة مقسـمة إلى أربعـة أجـزاء, الجـزء الأول يتحـدث فيـه عـن تـداول المعلومات، والجزء الثاني عن المعلومات والحكومة، والجزء الثالث بشأن المستندات الإلكترونية، أما الجزء الرابع فهو عن عقود نقل البضائع وسند الشحن الإلكتروني.

(2) "Electronic " include created, recorded , transmitted , or stored in digital form or in other intangible form by electronic , magnetic or optical means or by any other means that has capabilities for creation ,recording, transmission, or storage similar to those means part1article 1/a electronic commerce act.
Ravi Kalakota & Andrew B. Whinstone, Frontiers of electronic commerce , op,cit ,p234 =

وقد أصدرت كندا العديد من القوانين في هذا المجال، منها قانون التجارة الإلكترونية الموحد لعام 1999 السابق بيانه، وقانون المعلومات والمستندات الإلكترونية لسنة 2000، وقانون حماية البيانات الشخصية الصادر عام 2000، كما أصدرت العديد من الولايات قوانين محلية للتجارة الإلكترونية[1].

رابعًا: فرنسا:

عرف التقرير المقدم من مجموعة العمل المشكلة برئاسة السيد / لورنتز في يناير 1998 لوزير الاقتصاد الفرنسي التجارة الإلكترونية بأنها باختصار: " مجموعة المعاملات الرقمية المرتبطة بأنشطة تجارية بين المشروعات بعضها البعض، وبين المشروعات والأفراد، وبين المشروعات والإدارة ".

ويعد هذا التعريف موسعًا للتجارة الإلكترونية، حيث يرى أن المعاملات الرقمية المرتبطة بأنشطة تجارية تشمل الأنشطة البنكية باعتبار أنها تساهم في إبرام المعاملات التجارية عن طريق أنظمة الدفع الإلكتروني، فالتجارة الإلكترونية تشمل تبادل المعلومات، والمعاملات التجارية المتعلقة بالمعدات والمنتجات، وأيضًا تشمل الخدمات مثل خدمات المعلومات، والخدمات المالية والقانونية[2].

= عرف الإلكترون في اللغة العربية بأنه " جسيمات دقيقة ذات شحنة كهربائية سالبة، شحنتها هي الجزء الذي لا يتجزأ من الكهربائية " راجع في ذلك المعجم الوجيز، مجمع اللغة العربية، طبعة 1993، ص 23.

(1) من الولايات الكندية التي لديها قوانين للتجارة الإلكترونية كساسكاتشيفان ونيوفوندلاند ومانيتوبا وألبرتا ويوكون وبرينس إدوارد آيلاند وأونتاريو ونوفا سكوتيا.

(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 12.

ولتسهيل عملية التعاقد الإلكتروني في فرنسا تمت صياغة نوعين من العقود[1]، هـذه العقـود تتعلق بالتجارة الإلكترونية ومتصلة بها بغـرض تسـهيل المعـاملات، الأول هـو العقـد النمـوذجي للتجارة الإلكترونية بين التجار والمستهلكين، ويهدف إلى حماية المستهلكين مـن التعسـف، والثـاني هو العقود الخاصة بالمراكز التجارية الافتراضية.

ولم يكتف المشرع الفرنسي بإصدار قانون رقم 2000/230، ولكن تدخل بمقتضى المرسوم رقم 2001/741 والذي حـاول مـن خلالـه وضـع تنظـيم شـامل للتعاقـد الإلكـتروني في ضـوء التوجيـه الأوروبي رقم 97/7 بشأن حماية المستهلك في التعاقد عن بعُد، وكذلك بالقانون رقـم 2001/1062 المتعلق بالسلامة اليومية، وبذلك تكاد منظومة التشريعات الفرنسية تكتمل أكثر من غيرها فـيما يتعلق بالتنظيم التشريعي للتجارة الإلكترونية[2].

وقد صدر قـانون التوقيـع الإلكـتروني رقـم 230 لسـنة 2000 في 13 مـارس 2000, في صـورة تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي بما يجعلها متوافقـة مـع المعلوماتيـة, وقد أدرج هذا التعديل في نص المادة 1316 من القـانون المـدني الفرنسيـ في سـت فقـرات, ولقـد كرس هذا القانون مبدأين أساسيين: الأول ينصرف إلى عدم التمييـز بـين الكتابـة المعـدة للإثبـات بسبب الدعامة التي تـتم عليهـا والوسـيط الـذي تـتم مـن خلالـه, والثـاني ينصرـف إلى المسـاواة الوظيفية بين المحرر الإلكتروني

(1) د. أسامة أبو حسن مجاهد، خصوصية التعاقد عبر الإنترنت، مرجع سابق، ص 28 وما بعدها.
(2) د. هدى حامد قشقوش, الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 12.

والتوقيع الإلكتروني وبين المحرر العرفي والتوقيع التقليدي[1].

كما أن قانون العقوبات الفرنسي الجديد واكب المعلوماتية بنصه على قيام جريمة التزوير بأي وسيلة كانت Par quelques moyen, ليشمل التزوير المعلوماتي بجانب التزوير التقليدي, وتجريمه الاعتداء على المواقع الإلكترونية والأنظمة بالدخول والبقاء غير المشروع, وإعاقة تشغيل نظام المعالجة الآلية للمعطيات, وتدمير البيانات والمعطيات الإلكترونية.

كما أصدرت فرنسا في 21 يونيو 2004 قانونًا يتعلق بالثقة في الاقتصاد الرقمي.

خامسًا: لوكسمبورج:

صدر قانون التجارة الإلكترونية لدوقية لوكسمبورج، والذي تمت الموافقة عليه في 12 يوليو 2000 خاليًا من أي تعريف للتجارة الإلكترونية[2]، على الرغم من أن مشروع قانون التجارة الإلكترونية عرف في مادته الأولى المخصصة للتعريفات التجارة الإلكترونية بأنها: " كل استعمال لوسيلة من وسائل الاتصال الإلكترونية لتجارة السلع والخدمات، باستثناء العقود المبرمة بطريق اتصال تليفوني شفهي أو باستخدام التصوير". كما صدر في 1 يونيو 2001 قانون متعلق بالتواقيع الإلكترونية، والدفع الإلكتروني، وإنشاء لجنة التجارة الإلكترونية.

سادسًا: إيطاليا:

على الرغم من إصرار جانب من الفقه الإيطالي على أن التجارة الإلكترونية تختلف عن البيع عن بُعد؛ وذلك لأن المستهلك في التجارة

(1) د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, مرجع سابق, ص 292.
(2) د. خالد ممدوح، إبرام العقد الإلكتروني، مرجع سابق، ص 25.

الإلكترونية لا يقف موقفا سلبيًا كما هو الشأن في البيع عن بُعد، وبناء على توجيهات البرلمان والمجلس الأوروبي رقم 97/7 في شأن حماية المستهلك في مجال العقود عن بُعد أصدر المشرع الإيطالي سنة 1999 قرارًا بقانون في شأن التجارة الإلكترونية[1].

سابعًا: اليابان:

أصدرت اليابان العديد من التشريعات التي يمكن وصفها بأنها مقدمة لتنظيم للتجارة الإلكترونية، وتحديدًا في ميدان حماية المعلومات وتنظيم قواعد شهادات ضمان صحة تبادل المعلومات، ولم تصدر اليابان حتى وقتنا هذا تشريعًا متكاملا للتجارة الإلكترونية، وكلفت هيئة حكومية عليا منذ عام 1996م بمهمة وضع الإطار القانوني والتقني والتنظيمي للتجارة الإلكترونية، وقد قسمت هذه الهيئة أعمالها إلى مرحلتين أنجزت الأولى منهما عام 1998[2]، ولا تزال تنجز بقية محتوى وموضوعات المرحلة الثانية، ويبدو أن التجربة اليابانية ستمثل أكثر التجارب العالمية دقة وشمولا، وتعكس حقيقة مهمة هي أن اتخاذ التدابير التشريعية لا يتم على عجل لكنه لا يحتمل التأخير أيضًا، وسيكون بلا شك نموذجًا مميزًا وشاملا، وإلى جانب الجهد التشريعي فقد اتخذت الحكومة إجراءات واسعة لتهيئة القطاعات العامة والخاصة لممارسة واسعة وناشطة للتجارة الإلكترونية، بالرغم من أن أنشطتها ليست غريبة على البيئة اليابانية التي تسود فيها أكثر من غيرها.

---

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 16.

(2) http:// www. Bakernet. Com\ ecommerce\ japan.t.htm

ثامنًا: الهند:

تقف الهند في مقدمة الدول التي تقوم بجهود حثيثة في شتى مجالات التجارة الإلكترونية، فقد أنشأت الهند واديًا إلكترونيًا يستضيف الآن كيانات الكمبيوتر والمعلوماتية العملاقة.[1]

كما نفذت الحكومة الهندية مشروعًا طموحًا بوضع مشروع قانون شامل يهدف إلى إعطاء المشروعية للاتصالات الإلكترونية ويعالج الجرائم الإلكترونية، وقد ذكرت لجنة القانون الإداري - تعليقًا على ذلك - أن وضع إطار قانوني في الموضع الصحيح أصبح ملحًا لتطوير التجارة الإلكترونية، ويجب الإسراع في تنفيذ مشروعات التجارة الإلكترونية، حيث يتحرك بقية العالم في هذا الاتجاه على نحو سريع [2].

وفي 9 يونيو 2000م أصدرت الهند قانون المعلوماتية رقم (21) لسنة 2000م والذي اعتمد بالأساس على القانون النموذجي للتجارة الإلكترونية الصادر عن لجنة التجارة الدولية التابعة للأمم المتحدة (الأونسيترال)[3].

---

(1) وقعت الهند صفقة بقيمة 50 مليار دولار مع اليابان لإقامة ممر صناعي إلكتروني يربط بين العاصمة الهندية دلهي ومومباي، على مثال خطوط الحزام الصناعي، الذي يصل طوكيو بأوساكا، والذي يعمل بنجاح منذ 30 عاما، والذي يقال: إنه أسهم في ثلثي إجمالي الناتج المحلي لليابان، وسيشيد ممر دلهي مومباي، الذي يبلغ طوله 1483 كلم، خلال سبع سنوات، ليغطي منطقة يسكن فيها 180 مليون نسمة، وفيه ثلاثة موانئ وستة مطارات، ومشروع طاقة كهربائية بقوة أربعة آلاف ميجاوات. كما يحسب للحكومة الهندية اهتمامها الكبير بقطاع التكنولوجيا والتجارة الالكترونية.

(2) http: \\ www. Asiasource. Org\news

(3) http: \\ www. Naavio.org\importlaws\itbill2000\preamble. Htm=

= INDIA، INFORMA TION TECHNOLOGY ACT OF 2000

This Act seeks to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as electronic commerce, which involve the use of alternatives to paper،based methods of communication and storage of information, (and) to facilitate electronic filing of documents with the Government agencies.. It establishes the legal validity and enforceability of digital signatures and electronic records, as well as secure digital signatures and secure electronic records. The Act also establishes the controller of Certifying Authorities and authorizes this position to fulfill the many duties contained within Chapter Viol the Finally, the Act establishes the Cyber Appellate Tribunal, as well as various technology،related criminal offenses.

Noteworthy Points:

Digital Signature: Means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 (using an asymmetric cryptosystem and hash function).

Effect of Electronic Signature: Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person then, notwithstanding anything contains in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manners may by prescribed by the Central Government.

Electronic Record: Means data, record or data generated image or sound stored, received or sent in an electronic form.

Effect of Electronic Record: Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have neon satisfied if such information or matter is: (a) rendered or made available in an electronic form; and (b) accessible so as to be usable for a subsequent reference.

Secure Electronic Record: Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record =

تاسعًا: ماليزيا:

أنشأت ماليزيا ممرًا إلكترونيًا يماثل ذلك الموجود في الولايات المتحدة، وضعت فيه كل صنوف صناعة وتجارة الإلكترونيات.

وقد أنجزت ماليزيا منذ عام 1997 قانونًا للتجارة الإلكترونية والجريمة الإلكترونية والاتصالات، الأمر الذي شكل بيئة مثالية للشركات من مختلف الجنسيات أن تعمل وأن تطور في مجال البرمجيات والتجارة الإلكترونية في ماليزيا. كما يعد من أهم القوانين الصادرة في ماليزيا أيضًا قانون التوقيع الإلكتروني الذي صدر عام 1997، وأصبح نافذًا في أكتوبر 1998[1]، وكذلك تم صياغة مشروع قانون التجارة الإلكترونية في

= from such point of time to the time of verification.

Secure Digital Signature: If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the lime it was affixed, was: (a) unique to the subscriber affixing it; (b) capable of identifying such subscriber; (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature.

Certifying Authority: Means a person who has been granted a license to issue a Digital Signature certificate under section 24 (issue of certificates by Controller).

Treatment of Certification Authorities: This Act authorizes the Central Government to appoint a Controller of Certifying Authorities. The duties of the Controller are listed under Chapter VI of the Act, and include exercising supervision over the activities of certification authorities and delineating the duties of these certification authorities.

(1) http://www. Bakernet.com\ecommerce\Malaysia.t.summary. Htm
MALA YSIA DIGITA: SIGNA TURE BILL 1997:
Effective October 1 1998.

العام 2006.

This bill establishes the legal validity, enforceability and admissibility of digital signatures, It recognizes repositories and authorizes the Minister to appoint the Controller of Certification Authorities, Additionally, the bill addresses the functions of certification authorities, the general requirements for a licensed certification authority, and the application prettification authorities to annual performance audits, Finally, the bill delineates requirements for the issuance, suspension and revocation of a certificate.

Noteworthy Points:

Digital Signature: Means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer s public key can accurately deuterium: (a) whether the transformation was created using the private key that corresponds to the signer s public key; and (b) whether the message has been altered since the transformation was made.

Effect of Digital Signature: Where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that Eula shall be satisfied by a digital signature where: (a) that digital signature is verified by reference to the pubic key listed in a valid certificate issued by a licensed certification authority; (b) that digital signature was affixed by the signer with the intention of signing the message; and (c) the recipient has no knowledge or notice that the signer، (i) has breached a duty as a subscriber, or (ii) does not rightfully hold the private key used to affix the digital signature.

Certification Authority: Means a person who issues a certificate.

Certificate: Means a computer،based recode which: (a) identifies the certification authority issuing it; (b) names or identifies its subscriber; (c) contains the subscriber s public key; and (d) is digitally signed by the certification authority issuing it.

Treatment of Certification Authorities: The Minister shall appoint a Controller of Verification Authorities for the purposes of this Act, in particular for the purpose of monitoring an overseeing the activities of certification authorities. Additionally, the Minister is authorized to prescribe the qualification requirements for certification authorities under the Act.

عاشراً: سنغافورة:

اعتمدت سنغافورا القانون النموذجي للتجارة الالكترونية المعد من قبل اليونسترال , وذلك في عام 1999 حينما أصدرت قانون التجارة الالكترونية، وجاء مطابقا للقانون النموذجي، ونظم مسائل تبادل المعلومات وحمايتها وحجية التواقيع الالكترونية، والقواعد الاجرائية اللازمة لممارسة التجارة الالكترونية بكافة صورها، وتتميز سنغافورة بانها لم تعتمد النموذج القانوني الموحد دون مقاربته مع واقعها، فان كان صحيحا انها سنت القانون على نحو مطابق مع النموذج، الا ان ذلك استند الى دراسات بحثية شاملة ومشاركة واسعة بين قطاعات التجارة والصناعة والخدمات والقطاعات الحكومية امتدت على مدى الاعوام من1997 وحتى 1999، ويظهر اثر هذه الدراسات في الانظمة التنفيذية التي سنت مترافقة مع القانون، فهي انظمة اجرائية تفصيلية سدت نقاط النقص التي لا يغطيها القانون النموذجي وفسرت قواعده العامة واحالتها الى آليات تطبيق عملية تناسبت مع نتائج الدراسات والتوصيات التي اطلقتها الجهات المعنية في الدولة وفي مقدمتها القطاع الخاص.(1)

المطلب الثاني

التجارة الإلكترونية في التشريعات العربية

رغم أن التشريعات العربية معظمها خال من تنظيم التجارة الإلكترونية إلا أنه وجدت محاولات خجولة لبعض الدول العربية بسن مشروعات قوانين للتجارة الإلكترونية، كما أن هناك بعض الدول التي اتخذت خطوات جريئة وأصدرت قوانين خاصة بالمعاملات التجارية الإلكترونية ومنها

(1) يونس عرب - التجارة الالكترونية - المرجع السابق - ص 35.

تونس، والإمارات العربية المتحدة، والأردن، ومملكة البحرين، وسلطنة عمان.

أولا: الجمهورية التونسية:

تعتبر الجمهورية التونسية من أوائل الدول المنظمة للتجارة الإلكترونية على مستوى الوطن العربي، حيث كان لتونس السبق في إصدار قانون خاص بالتجارة الإلكترونية تحت رقم 83 لسنة 2000، ووفقا لهذا القانون تخضع العقود الإلكترونية لنظام العقود الكتابية من حيث التعبير عن الإرادة، وأثرها القانوني، وصحتها وقابليتها للتنفيذ فيما لا يتعارض وأحكام هذا القانون، ويتضمن القانون تنظيمًا لأحكام الوثيقة الإلكترونية، والإمضاء الإلكتروني، وكيفية التعامل بهما، واتخاذ الاحتياطيات اللازمة لتفادي كل استعمال غير مشروع لعناصر التشفير أو المعدات الشخصية المتعلقة بالإمضاء، وقد عرف المشرع التونسي التجارة الإلكترونية بأنها: "العمليات التجارية التي تتم عبر المبادلات الإلكترونية" وعرفت المبادلات الإلكترونية بأنها: "المبادلات التي تتم باستعمال الوثائق الإلكترونية". ولكن يلاحظ أن هذا التعريف لم يبين الوسائل الإلكترونية التي يتم عن طريقها التعاقد عن بُعد.

ويتضح من تعريف التجارة الإلكترونية أنها عملية تجارية، سواء أكان موضوعها سلعة أو خدمة أو أداء عمل، تتم عن طريق المبادلات الإلكترونية، وذلك لأن أي عملية تجارية هي مبادلة ما بين سلعة أو خدمة أو أداء عمل ولكن بطريقة إلكترونية.[1]

(1) وافق مجلس النواب التونسي على هذا القانون في 27 يوليو 2000 وصدر في 9 أغسطس 2000 ونشر في جريدة الرائد الرسمي للجمهورية التونسية في 11 أغسطس 2000.

ثانيًا: دولة الإمارات العربية المتحدة:

دولة الإمارات العربية المتحدة من أول الدول في المنطقة العربية التي بدأت بتحديث البنية التحتية الخاصة بقطاع الاتصالات تمهيدًا للدخول بقوة إلى سوق التجارة الإلكترونية، فبالنظر إلى شبكة الاتصالات الحديثة والقوة الاقتصادية الهائلة التي تملكها، وتدني نسبة الأمية فيها، وتحديث تشريعاتها التي جعلتها في مصاف الدول المنفتحة على العالم، كل ذلك ساهم في جعلها مركزًا متقدمًا للمال والأعمال، ومن ثم دخولها إلى التجارة الإلكترونية بقوة، سواء على مستوى الاتحاد أو حكومات الإمارات المحلية، كما هو الشأن لدى حكومة إمارة دبي.

وكان لإنشاء مؤسسة كومترست ضمن مؤسسة الاتصالات[1] وقيام دولة الإمارات العربية ضمن منظومة دول مجلس التعاون الخليجي بالتوقيع على الإعلان المشترك بالأحرف الأولى مع الولايات المتحدة عام 2001، تمهيدًا لإبرام اتفاقية في شأن التبادل التجاري الإلكتروني، وكذلك قيام بعض الحكومات المحلية بإنشاء مناطق حرة مثل المنطقة الحرة في إمارتي أبو ظبي ودبي.

(1) وقد أعلنت مؤسسة الإمارات للاتصالات (اتصالات) عن إنشاء وحدة أعمال إلكترونية تعمل كمنفذ متكامل لجميع الخدمات الإلكترونية، بعد دمج اثنتين من أهم وحدات الأعمال التابعة لها، وهما "وحدة الإمارات للإنترنت والوسائط المتعددة" و"كومترست". وستعرف الوحدة الإلكترونية الجديدة باسم "Company.e" وهي تؤدي إلى الاستفادة من الاقتصاد الرقمي في دولة الإمارات وفي كافة أرجاء المنطقة، وتقديم الخدمات الإلكترونية، وعروض شبكة الإنترنت، وخدمات القيمة المضافة، واستشارات تقنية المعلومات والاتصالات وإدارة المشروعات، بما يؤدي إلى تعزيز حجم ونطاق المبيعات، ولتلبية احتياجات تقنية المعلومات والاتصالات ودخول كافة أسواق المنطقة.

وقد خطت إمارة دبي خطوات واسعة نحو التجارة الإلكترونية، فهناك سوق دبي الإلكترونية[1]، وهناك كذلك الحكومة الإلكترونية في إمارة دبي التي تم الإعداد لها اعتبارًا من أبريل عام 2000، وقد دخلت حيز التنفيذ مع بداية عام 2003.

وقد جاءت دولة الإمارات العربية المتحدة في مقدمة الدول العربية في ممارسة التجارة الإلكترونية، حيث كانت من الدول العربية الأوائل التي قامت بتنظيم هذه التجارة تشريعيًا، وليس أدل على ذلك مما قامت به حكومة دبي بإصدار القانون رقم 2 لسنة 2002 بشأن المعاملات والتجارة الإلكترونية والذي جاء في مقدمته أنه جاء تحقيقًا لتوجه حكومة دبي بإحلال وسائل التقنية الحديثة في المعاملات والتبادل التجاري,[2]وقبل صدور هذا القانون صدر القانون رقم 1 لسنة 2000 في شأن منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام , وكان الهدف من ذلك القانون تهيئة المناسبة لتطبيق قانون التجارة الإلكترونية عند صدوره[3].

(1) صدر المرسوم الحكومي بإنشاء المنطقة الحرة بدبي بتاريخ 31 يناير 2000 بهدف إنشاء منطقة حرة تعرف باسم منطقة دبي الحرة للتكنولوجيا والتجارة الإلكترونية والإعلام، وهي هيئة اعتبارية لها استقلالها المالي والإداري، وموقعها في المنطقة الحرة الواقعة في جبل علي.

(2) أصدر الشيخ مكتوم بن راشد آل مكتوم حاكم إمارة دبي رحمه الله هذا القانون في دبي بتاريخ 12 فبراير 2002 الموافق 30 ذي القعدة 1422.

(3) جاء في كتاب رؤيتي للشيخ محمد بن راشد آل مكتوم: إن دبي تتمتع بالإمكانات الكفيلة بتوفير الظروف المناسبة لنجاح الأعمال في الاقتصاد الجديد، فلدينا خبرة مشهود لها عالميًا في مجال التجارة الدولية, وبنية عمرانية وأساسية على أعلى المستويات العالمية, وأحدث المقومات التكنولوجية التي تتجسد في إنشاء أول منطقة حرة في الشرق الأوسط للتجارة الإلكترونية هي مدينة دبي للإنترنت والتكنولوجيا والاعلام التي افتتحت في أكتوبر 2000. =

وقد جاء قانون المعاملات والتجارة الإلكترونية في 39 مادة مقسمة على ثمانية فصول، وباستعراض أحكام هذا القانون يتبين أن واضع قانون إمارة دبي قد تبنى في أحكام هذا القانون تلك الأحكام الواردة في القانون النموذجي للأمم المتحدة في شأن التجارة الإلكترونية والذي أعدته لجنة القانون التجاري الدولي بالمنظمة "أونسيترال" وصدر عن الجمعية العامة للأمم المتحدة عام 1996، وقد برز هذا التلاقي ما بين قانون إمارة دبي، والقانون النموذجي للأمم المتحدة في موضوعات عديدة منها عملية إرسال واستقبال الرسالة الإلكترونية، وكيفية حفظها واسترجاعها، والأحكام الخاصة بزمان الإرسال والاستقبال، توصلا إلى تحديد القانون الواجب التطبيق على عقد التجارة الإلكترونية، وكذلك الاختصاص القضائي للمحاكم التي تنظر الدعاوى الناشئة عن تطبيق أحكام هذا القانون.

بالإضافة إلى ما تقدم فقد تضمن القانون الأحكام الخاصة بمزودي خدمة شبكة الإنترنت، ومدى حجية الشهادات الإلكترونية الصادرة عنهم، والمسئولية القانونية التي تنظم عمل هؤلاء في حال إخلالهم بالواجبات المفروضة عليهم.

وجاءت الأحكام المنظمة للتوقيع الإلكتروني مشابهة إلى حد ما للأحكام

= لكن رغم كل ما حققناه لا نزال في حاجة إلى تعزيز جودة كل الخدمات إذا أردنا أن نتبوأ مركزًا قياديًا في الاقتصاد الجديد، هذا هدف ألتزم به وأسعى شخصيًا إلى تحقيقه, وهناك هدف آخر لا يقل أهمية هو أن تحقق دبي مركزًا رياديًا متميزًا في مجال الأعمال المتصلة بالاقتصاد الجديد ليس على المستويين المحلي والاقليمي فقط, بل على مستوى العالم, لذا سنعمل دائمًا أن يجد مجتمع الأعمال في دبي ما لا يجده في أي مكان آخر في العالم.

للمزيد انظر: محمد بن راشد آل مكتوم, رؤيتي التحديات في سباق التميز, مرجع سابق, ص 25.

الواردة بهذا الشأن في القانون النموذجي للأمم المتحدة، وذلك فيما يتعلق بأحكام التوقيع وحجيته في الإثبات، وكذلك شهادات المصادقة التي تتعلق بذلك التوقيع[1]، كما تضمن قانون المعاملات والتجارة الإلكترونية 2002/2 نظم آلية التعاقد الإلكتروني بالاستناد إلى المراسلات الإلكترونية والكتابة الإلكترونية والتوقيع الإلكتروني، وبيّن كيفية حفظ السجلات أو المستندات الإلكترونية، ومتى تكون هذه المستندات أصلية، وقرر قبول مخرجات الوسائل الإلكترونية الحديثة، ومنحها الحجية في الإثبات، وقد عرف المشرع التجارة الإلكترونية في الفصل الأول المخصص للتعريفات بأنها: " المعاملات التجارية التي تباشر بواسطة المراسلات الإلكترونية"[2].

وفي2006/1/30 صدر القانون الاتحادي رقم 2006/1 في شأن المعاملات والتجارة الإلكترونية[3]، في عشرة فصول متضمنا 37 مادة، وقد خصص الفصل الأول للتعاريف، وفيه عرف التجارة الإلكترونية بأنها: "المعاملات الإلكترونية التي تباشر بواسطة الوسائل الإلكترونية"، وتضمن الفصل الثالث من القانون متطلبات المعاملات الإلكترونية، وهي المراسلات الإلكترونية، حفظ السجلات الإلكترونية، قبول التعامل الإلكتروني، الكتابة، التوقيع الإلكتروني، الأصل الإلكتروني، قبول وحجية البيانات الإلكترونية، وتضمن الفصل الرابع إنشاء العقود وصحتها، والمعاملات الإلكترونية

(1) د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص 106.

(2) تناول القانون متطلبات المعاملات الإلكترونية، والعقود الإلكترونية وحجيتها، والتوقيعات الإلكترونية، وخدمات التصديق.

(3) صدر هذا القانون في 30 يناير 2006 م، الموافق 30 من ذي الحجة 1426 هـ وجاء مشابها لقانون إمارة دبي في معظم مواده.

المؤتمتة، والإسناد أي صدور الرسالة الإلكترونيـة عـن المنشـئ، والعلاقـة بينـه وبـين المرسـل إليـه، والإقرار بالاستلام بمعنى أن يكون المرسل إليه قد أخطر المنشئ باستلام الرسالة الإلكترونية، وزمان ومكان إرسال واستلام الرسائل الإلكترونية، وجاء الفصل الخامس متضمنًا إجراءات التوثيـق سـواء منها ما هو منصوص عليه في القانون، أو متفق عليه بـين الطـرفين، أو المعقولـة تجاريًـا، فتضـمن هذا الفصل السجلات الإلكترونية المحمية، والتوقيع الإلكتروني المحمي، كـما جـاء القـانون مؤكـدًا على ضرورة أن يكون التوقيع الإلكتروني معززًا بشهادة مصـادقة إلكترونيـة، وهكـذا جـاء الفصـل السادس متضمنًا الأحكام المتصلة بشهادات المصادقة الإلكترونية وخدمات التصديق، كـما تضـمن الفصل السابع الاعتراف بشهادات المصادقة الإلكترونية والتوقيعات الإلكترونية الأجنبيـة، في حـين أن الفصل الثامن نص على الاستخدام الحكومي للسجلات والتوقيعـات الإلكترونيـة، وأمـا الفصـل التاسع فقد شمل كافة العقوبات التي قررها المشرع الإماراتي في حالـة مخالفـة نصـوص القـانون المنظم لها، وجاء الفصل العاشر متضمنًا الأحكام الختاميـة وهـي تلـك الخاصـة بالإصـدار وإلغـاء الأحكام المخالفة والنشر.

ثالثًا: الأردن:

يعتبر قانون المعاملات الإلكترونية الأردني رقـم 85 لسـنة2001[1] مـن القـوانين المهمـة التـي عالجت العديد من القضايا ذات الصلة بالتجـارة الإلكترونيـة، ويهـدف هـذا القـانون إلى تسـهيل استعمال الوسائل الإلكترونية في

(1) نشر هذا القانون في الجريدة الرسمية الأردنية في العدد رقـم 4534 بتـاريخ 31 /12 /2001، ويتكـون هـذا القانون من 41 مادة تناولت بيان ماهية المعاملات الإلكترونية، والعقد الإلكتروني، والسندات الإلكترونية القابلة للتحويل، وتوثيق السجل، والتوقيع الإلكتروني.

إجراء المعاملات، وذلك مع مراعاة أحكام أي قوانين أخرى ودون تعديل أو إلغاء لأي من هذه الأحكام، كما يراعى عند تطبيق أحكام هذا القانون قواعد العرف التجاري الدولي ذات العلاقة بالمعاملات الإلكترونية ودرجة التقدم في تقنية تبادلها، ويسري هذا القانون على المعاملات الإلكترونية، والسجلات الإلكترونية، والتوقيع الإلكتروني، وأي رسالة معلومات إلكترونية، وعلى المعاملات الإلكترونية التي تعتمدها أي دائرة حكومية أو مؤسسة رسمية بصورة كلية أو جزئية.

كما نص على أن تطبق أحكام هذا القانون على المعاملات التي يتفق أطرافها على تنفيذ معاملاتهم بوسائل إلكترونية، ما لم يرد فيه نص صريح يقضي بغير ذلك، ولمقاصد هذه المادة لا يعتبر الاتفاق بين أطراف معينة على إجراء معاملات محددة بوسائل إلكترونية ملزمًا لإجراء معاملات أخرى بهذه الوسائل.

ولم يضع قانون المعاملات الإلكترونية الأردني تعريفًا للتجارة الإلكترونية، ولكنه عرف المعاملات بأنها إجراء - أو مجموعة من الإجراءات - يتم بين طرفين أو أكثر، لإنشاء التزامات على طرف واحد، أو التزامات تبادلية بين أكثر من طرف، ويتعلق بعمل تجاري أو التزام مدني أو بعلاقة مع أي دائرة حكومية، كما عرف المعاملات الإلكترونية بأنها المعاملات التي تنفذ بوسائل إلكترونية، ووضع القانون تعريفًا للإلكتروني بأنه تقنية استخدام وسائل كهربائية أو مغناطيسية أو ضوئية أو إلكترومغناطيسية أو أي وسائل مشابهة في تبادل المعلومات وتخزينها0

واستثنى من تطبيق أحكام هذا القانون ما يلي:

أ) العقود والمستندات والوثائق التي تنظم وفقًا لتشريعات خاصة بشكل معين، أو تتم بإجراءات محددة ومنها:

1) إنشاء الوصية وتعديلها.

2) إنشاء الوقف وتعديل شروطه.

3) معاملات التصرف بالأموال غير المنقولة، بما في ذلك الوكالات المتعلقة بها، وسندات ملكيتها، وإنشاء الحقوق العينية عليها، باستثناء عقود الإيجار الخاصة بهذه الأموال.

4) الوكالات والمعاملات المتعلقة بالأحوال الشخصية.

5) الإشعارات المتعلقة بإلغاء أو فسخ عقود خدمات المياه والكهرباء والتأمين الصحي والتأمين على الحياة.

6) لوائح الدعاوى والمرافعات، وإشعارات التبليغ القضائية، وقرارات المحاكم.

ب) الأوراق المالية إلا ما تنص عليه تعليمات خاصة تصدر عن الجهات المختصة استنادًا لقانون الأوراق المالية النافذ المفعول.

كما نظم القانون السجل والعقد والرسالة والتوقيع الإلكتروني، والسند الإلكتروني القابل للتحويل، والتحويل الإلكتروني للأموال، وتوثيق السجل والتوقيع الإلكتروني.

وقد وضع القانون عقوبات لكل من يقوم بإنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالي أو لأي غرض غير مشروع، ولكل من يقدم إلى جهة تمارس أعمال توثيق المستندات معلومات غير صحيحة بقصد إصدار شهادة توثيق أو وقف سريانها أو إلغائها، وعاقب أي جهة تمارس أعمال توثيق المستندات إذا قامت بتقديم معلومات غير صحيحة في طلب التسجيل، أو أفشت أسرار أحد عملائها، أو خالفت الأنظمة والتعليمات التي تصدر استنادًا إلى هذا القانون، وعاقب كل من يرتكب فعلا يشكل جريمة بموجب التشريعات النافذة بواسطة استخدام الوسائل الإلكترونية، ويعاقب بالعقوبة

الأشد إذا كانت العقوبات المقررة في تلك التشريعات تزيد على العقوبة المقررة في هذا القانون.

رابعًا: مملكة البحرين:

تعد دولة البحرين من أوائل الدول العربية التي أصدرت قانونا للمعاملات الإلكترونية وذلك بالمرسوم بقانون رقم (28) لسنة 2002 بشأن المعاملات الإلكترونية، وقد بدأ هذا القانون بوضع تعاريف لبعض المصطلحات ليس من بينها التجارة الإلكترونية، ونص على أن تسري أحكام هذا القانون على السجلات والتوقيعات الإلكترونية.

واستثنى من تطبيق أحكام القانون ما يلي:

أ) كافة المسائل التي ينعقد الاختصاص بشأنها للمحاكم الشرعية.

ب) مسائل الأحوال الشخصية لغير المسلمين، مثل الزواج والطلاق والحضانة والتبني والميراث وإنشاء الوصايا وتعديلها.

ج) المعاملات والتصرفات التي يشترط القانون للاعتداد بها أن تكون مثبتة في محررات رسمية.

د) السندات القابلة للتداول.

هـ) سندات الملكية، فيما عدا تلك المنصوص عليها في المادة (20) من هذا القانون[1].

---

(1) نصت المادة (20) على مستندات نقل البضائع بقولها:
1- تسري أحكام هذه المادة بشأن أي إجراء يتعلق بعقد نقل البضائع، بما في ذلك الآتي:
أ- الإخطار بعلامات أو عدد أو كمية أو وزن البضائع.
ب- تحديد نوع البضائع أو قيمتها، أو الإقرار بذلك.
ج- إصدار إيصال بتسلم البضائع.
د- إصدار تأكيد بأن البضائع قد تم تحميلها.
هـ- إصدار تعليمات لناقل البضائع. =

= و- المطالبة بتسليم البضائع.
ز- الإذن بالإفراج عن البضائع.
ح- الإخطار بفقد البضائع أو تلفها.
ط- التعهد بتسليم البضائع إلى شخص معين أو إلى شخص مفوض بالمطالبة بالتسليم.
ى- منح أو اكتساب أو نقل أو تداول أية حقوق بشأن البضائع، أو التخلي أو التنازل عن أي من هذه الحقوق.
ك- الإخطار بشروط عقد نقل البضائع.
ل- الإخطار أو الإفادة بتنفيذ عقد نقل البضائع.
م- اكتساب أو نقل الحقوق والالتزامات التي ينص عليها عقد نقل البضائع.

2- إذا تطلب القانون أن يتم أي إجراء مما نص عليه في البند السابق عن طريق مستند مكتوب، فإن استيفاء ذلك من خلال استعمال سجل إلكتروني أو أكثر يفي بمتطلبات هذا القانون.

3- مع عدم الإخلال بنص البند السابق، فإنه إذا اشترط القانون لمنح أي حق أو لإسناد أي التزام أن يتم من خلال استعمال أو تسليم مستند مكتوب، فإن استيفاء ذلك من خلال استعمال سجل إلكتروني أو أكثر يفي بمتطلبات هذا القانون، بشرط أن يتم إنشاء تلك السجلات بطريقة تضمن أن يكون الحق أو الالتزام مقصورًا على الشخص المعني دون سواه.

4- يراعى بشأن تقدير مدى كفاءة طريقة إنشاء هذه السجلات في تحقيق الضمان المشار إليه في البند السابق، الشروط التي اتفق عليها الأطراف، وكافة الظروف والملابسات، بما في ذلك الغرض الذي تم من أجله الإخطار بالحق أو الالتزام.

5- إذا استعمل سجل إلكتروني أو أكثر لأي من الإجراءات المنصوص عليها في الفقرتين (ي) أو(م) من البند(1) من هذه المادة، فإنه لا يعتد بأي مستند خطي في هذا الشأن إلا إذا تحقق الشرطان الآتيان:
أ- العدول عن استعمال السجلات الإلكترونية بشأن ذلك الإجراء، سواء تم ذلك بالاتفاق بين الأطراف المعنيين أو بإرادة أحدهم.
ب- أن يتضمن المستند الخطي البديل ما يفيد العدول عن استعمال السجلات الإلكترونية في هذا الشأن.
=

كما نص القانون على قبول التعامل الإلكتروني، وشروط قبول الجهات العامة للتعامل الإلكتروني، وحجية السجلات الإلكترونية في الإثبات، والتوقيع الإلكتروني، والمستندات الأصلية، واشتراط تقديم نسخة واحدة أو أكثر من مستند، وحفظ المستندات، وإبرام العقود، وإبداء النوايا أو التعبيرات المشابهة، وحدد دور الوكلاء الإلكترونيين في إبرام العقود، والإسناد، ووضح الإقرار بتسلم السجل الإلكتروني، وحدد وقت ومكان إرسال وتسلم السجلات الإلكترونية، ونص على اعتماد مزودي خدمة الشهادات، وحالات إلغاء اعتمادهم، واعتماد مزودي خدمة الشهادات الخارجيين، وإلغاء اعتمادهم، ومسئولية مزودي خدمة الشهادات المعتمدين، ومسئولية وسطاء الشبكات، ومستندات نقل البضائع، وتسجيل أسماء النطاق، والطعن في صحة السجلات والتوقيعات الإلكترونية، وسلطة التفتيش، والعقوبات، ومسئولية الشخص الاعتباري وموظفيه.[1]

خامسًا: سلطنة عمان:

صدر في سلطنة عمان قانون المعاملات الإلكترونية في العام 2008[2]، والمكون من 54 مادة مقسمة على تسعة فصول، حدد نطاق تطبيقه، والمبدأ

=6- لا يترتب على استبدال المستندات الخطية بسجلات إلكترونية على النحو المنصوص عليه في البند السابق التأثير على أي من حقوق أو التزامات الأطراف المعنيين.

7- لا يترتب على مجرد ورود عقد نقل البضائع في سجل إلكتروني أو أكثر، أو ثبوته عن طريق سجل إلكتروني أو أكثر، بدلا من المستندات الورقية، المساس بأحكام القوانين ذات العلاقة بعقد النقل وسريانها على هذا العقد.

(1) صدر هذا القانون بتاريخ 7 رجب 423 هـ الموافق 14 سبتمبر 2002 م، وتم تطبيقه والعمل به في 14 ديسمبر 2002.

(2) صدر قانون المعاملات الإلكترونية وفقًا للمرسوم السلطاني رقم 2008/69م.

في قبول التعامل به، فهو من زاوية أولى حصر نطاقه على السجلات والتوقيعات الإلكترونية التي تتعلق بالمعاملات الإلكترونية كقاعدة عامة، وأورد عليها بعض الاستثناءات المحددة بنص القانون، ومن زاوية أخرى نجد أن قبول حكم القانون وسريانه على الشخص في نطاق التعاملات الإلكترونية قد يستفاد صراحة أو ضمنًا، كما أنه يجوز الاتفاق على مخالفة حكم هذا القانون بين أطراف العلاقة التعاقدية، وفيما يتعلق بالاستخدام الحكومي للسجلات والتوقيعات الإلكترونية فإننا نجد أن القانون لا يسري على الحكومة في المعاملات التي تكون طرفًا فيها، إلا بموافقة صريحة منها.

وتنص الفقرة الأولى من المادة الثالثة من القانون على أنه: " تسري أحكام هذا القانون على المعاملات والسجلات والتوقيعات الإلكترونية، كما تسري على أية رسالة معلومات إلكترونية".

والواضح من النص السابق أن قانون المعاملات الإلكترونية جاء ليحكم المعاملات والسجلات والتوقيعات ورسائل المعلومات الإلكترونية، والمعاملة الإلكترونية هي كما عرفها القانون في المادة الأولى منه: أي إجراء أو عقد يُبرم أو يُنفَذ كليًا أو جزئيًا بواسطة رسائل إلكترونية. أما السجل الإلكتروني فيقصد به العقد أو القيد أو رسالة المعلومات التي يتم إنشاؤها أو تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو تسلمها بوسائل إلكترونية على وسيط ملموس أو أي وسيط آخر، ويكون قابلا للتسلم بشكل يمكن فهمه.

أما التوقيع الإلكتروني فيقصد به التوقيع على رسالة أو معاملة إلكترونية في شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متفرد يسمح بتحديد شخص الموقّع وتمييزه عن غيره.

والجدير بالذكر أن ثمة شروطًا اشترط القانون توافرها في التوقيع الإلكتروني ليكون جديرًا بالحماية القانونية، فنص في المادة 22 منه على أنه: " يعتبر التوقيع الإلكتروني محميًا وجديرًا بأن يعتمد عليه إذا تحقق الآتي:

أ) كانت أداة إنشاء التوقيع في سياق استخدامها مقصورة على الموقع دون غيره.

ب) كانت أداة إنشاء التوقيع في وقت التوقيع، تحت سيطرة الموقع دون غيره.

ج) كان ممكنًا كشف أي تغيير للتوقيع الإلكتروني يحدث بعد وقت التوقيع.

د) كان ممكنًا كشف أي تغيير في المعلومات المرتبطة بالتوقيع يحدث بعد وقت التوقيع.

ومع ذلك يجوز لكل ذي شأن أن يثبت بأية طريقة أن التوقيع الإلكتروني جدير بأن يعتمد عليه أو أنه ليس كذلك.

أما الرسالة الإلكترونية فيقصد بها: معلومات إلكترونية يتم إرسالها بوسائل إلكترونية أيًا كانت وسيلة استخراجها في المكان المستلمة فيه .

واستثناء من القاعدة العامة السالفة الذكر استثنى القانون بعض الأوضاع القانونية من نطاق سريان هذا القانون، وكل مخالفة في ذلك تبطل التصرف بطلانًا مطلقًا على اعتبار أن الشكلية ركن للانعقاد لا شرط للإثبات، وبعبارة أخرى لتعلقه بالنظام العام، وذلك لأن هذه الاستثناءات تمثل حالات لها خصوصية تقتضي عدم خضوعها لأحكام قاعدة خضوع المعاملات والسجلات والتوقيعات الإلكترونية، وهذه الاستثناءات هي :-

أ- المعاملات والأمور المتعلقة بقانون الأحوال الشخصية:

ويقصد بها كل الأمور والمعاملات التي تتعلق بالأحوال الشخصية كالزواج والطلاق والوصايا والهبات، وعلى هذا الأساس نجد أن عقدًا كعقد الزواج لا يدخل من ضمن العقود التي تسري عليها أحكام التوقيع الإلكتروني، وكذلك إشهار الطلاق، وأيضًا من التعاملات التي تخرج من نطاق التوقيع الإلكتروني تلك الخاصة بالوصايا بمفهومها الشرعي.

والعلة من إخراج المعاملات والأمور المتعلقة بقانون الأحوال الشخصية من نطاق تطبيق القانون كونها تصرفات شخصية بصفة محددة، هذا من جهة ومن جهة أخرى لخطورتها من الناحية الشرعية، وبالتالي فهي بحاجة إلى توثيق بطرق التوثيق التقليدية.[1]

ب- إجراءات المحاكم، والإعلانات القضائية، والإعلانات بالحضور، وأوامر التفتيش، وأوامر القبض، والأحكام القضائية.

والعلة من إخراج هذه المستندات من نطاق تطبيق هذا القانون أن لها طبيعة خاصة لأجل ذلك نجد أن المشرع ومن خلال قانون الإجراءات الجزائية وقانون الإجراءات المدنية والتجارية وضع لها ضوابط واشتراطات معينة لا بد وأن تستوفيها، مما يعني عدم إمكانية استعمال الوسائل الإلكترونية فيها خاصة في وقتنا الحالي، ومع ذلك فإننا نرى أنه في المستقبل ومع إنشاء ما يعرف بالمحكمة الإلكترونية وتطبيقها قد يمكن إنجاز المعاملات السابقة إلكترونيًا.

ج- أي مستند يتطلب القانون توثيقه بواسطة الكاتب بالعدل :

المستندات التي لا تتوافر حجيتها إلا بتصديق الكاتب بالعدل عليها،

---

(1) د. فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، مرجع سابق، ص 120.

وسواء ورد ذكرها في قانون الكاتب بالعدل أو أي قانون آخر تخرج من نطاق قانون المعاملات الإلكترونية.

ومن الأمثلة على هذه المستندات الوكالة بنوعيها العام والخاص الذي، والذي ينيب فيه الموكل آخر للقيام بتصرف قانوني كوكيل عنه سواء كان داخل الدولة أو خارجها، والعلة من إخراج هذه الفئة من نطاق تطبيق القانون تكمن في الطبيعة الخاصة لهذه المستندات، هذا من جهة ومن جهة أخرى هناك إجراءات وضوابط رسمها قانون الكاتب بالعدل للمستندات التي تتطلب التوثيق والتصديق من قبل الكاتب بالعدل، منها على سبيل المثال التأكد من شخصية ذوي الشأن ومن أهليتهم القانونية لإبرام التصرف[1].

كما نص القانون على مبدأ قبول التعامل الإلكتروني والذي تضمن قاعدة عامة وبعض الاستثناءات، وذلك على النحو التالي: القاعدة التي أتي بها القانون في هذا المجال هي أن الشخص لا يجبر على التعامل وفق أحكام القانون، ويترتب على هذا أن أحكام هذا القانون تطبق على الأطراف الذين اتفقوا على إجراء معاملاتهم بوسائل إلكترونية صراحة أو ضمنًا، بيد أنه يشترط أن يكون سلوك الشخص إيجابيًا في حالة الموافقة الضمنية، فالمادة الرابعة من القانون في الفقرة الأولى منها نصت على أنه: " تطبق أحكام هذا القانون على المعاملات التي تتم بين الأطراف الذين اتفقوا على إجراء معاملاتهم بوسائل إلكترونية، ويجوز استنتاج موافقة الشخص على ذلك من سلوكه ".

أما بالنسبة للحكومة فإنها إذا ما رغبت في التعامل الإلكتروني في المعاملات التي تكون طرفًا فيها وفق أحكام هذا القانون فإنه يجب أن تكون

(1) د. فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، مرجع سابق، ص 128.

موافقتها على هذا التعامل صريحة وليست ضمنية، ومؤدى ذلك أن الحكومة لا يفرض عليها التعامل في كافة معاملاتها وفق أحكام هذا القانون، ولكن لا بد وأن تقبل ذلك التعامل صراحة، وبالتالي فإنه لا يستفاد قبولها ضمنًا بناءً على مسلك إيجابي منها في شأن قبول ذلك التعامل؛ لأن الموافقة الضمنية بالنسبة للحكومة لم ينص عليها القانون في الفقرة الأولى من المادة 4 من القانون، بل اشترط الموافقة الصريحة، ويقصد بالحكومة حسب تعريفها الوارد في المادة الأولى من أحكام هذا القانون وحدات الجهاز الإداري للدولة وما في حكمها.

واستثناء من القاعدة السابقة فإنه يجوز للأطراف في المعاملة أو العقد الإلكتروني أن يتفقا على التعاقد بطريق تقليدي وليس بالطريق الإلكتروني المنصوص عليه في هذا القانون، وبالتالي خروج الأطراف من نطاق تطبيق أحكام هذا القانون، وعلى ذلك يجوز للأطراف الذين لهم علاقة بإنشاء أو إرسال أو تسلم أو تخزين أو معالجة سجلات إلكترونية الاتفاق على التعامل بصورة مغايرة لأي من أحكام هذا القانون، وتحديدًا القواعد الواردة في الفصول من الثاني حتى الرابع من هذا القانون.

أما الاستثناء الثاني من القاعدة السابقة ففحواه أن أي اتفاق يتم بين الأطراف لإنجاز معاملة معينة بوسائل إلكترونية لا يكون ملزمًا لأي منهم لإنجاز معاملات أخرى بذات الوسائل، وبالتالي فإن قيام شخص ما باستخدام الوسائل الإلكترونية لإنجاز معاملة ما لا يعني أنه ملتزم باستخدام ذات الأسلوب في إنجاز معاملة أخرى وإنما له الخيار.

وبخصوص العقوبات نجد أن المشرع العماني قد أورد عدة جرائم ووضع لها عقوبات، ومن هذه الجرائم:

1) من تسبب عمدًا في تعديل غير مرخص به في محتويات أي حاسب

آلي بقصد إضعاف فاعليته، أو منع أو تعويق الدخول إلى أي برنامج أو بيانات محفوظة فيه، أو إضعاف فاعلية ذلك البرنامج، أو إضعاف الاعتماد على تلك البيانات إذا تم ذلك التعديل بإحدى الطرق الآتية:

أ) شطب أي برنامج أو بيانات محفوظة في الحاسب الآلي.

ب) إضافة أي برنامج أو بيانات إلى محتويات الحاسب الآلي.

ج) أي فعل يسهم في إحداث ذلك التعديل.

2) اخترق جهاز حاسب آلي أو منظومة حاسبات آلية أو موقع على الإنترنت أو شبكة إنترنت وترتب على ذلك:

أ) تعطيل أنظمة تشغيل جهاز الحاسب الآلي أو منظومة الحاسبات الآلية.

ب) إتلاف برامج الحاسب الآلي أو الحاسبات الآلية وما تحتويه من معلومات.

ج) سرقة المعلومات.

د) استخدام المعلومات التي تتضمنها مخرجات الحاسبات الآلية في أغراض غير مشروعة.

هـ) إدخال معلومات غير صحيحة.

3) دخل بطريق الغش إلى نظام معلومات أو قاعدة بيانات بغرض العبث بالتوقيعات الإلكترونية.

4) قام بطريقة غير مشروعة بكشف مفاتيح لفض التشفير أو فض تشفير معلومات مودعة لديه.

5) استعمل بصفة غير مشروعة عناصر تشفير شخصية متعلقة بتوقيع غيره.

6) اخترق أو اعترض معلومات أو بيانات مشفرة أو قام بفض شفرتها عمدًا دون مسوغ قانوني، وتضاعف العقوبة إذا كانت المعلومات أو

البيانات تتعلق بسر من أسرار الدولة.

7) قام عمدًا بفض معلومات أو بيانات مشفرة بأية طريقة في غير الأحوال المصرح بها قانونًا.

8) قام عمدًا بإنشاء أو نشر شهادة أو زود بمعلومات إلكترونية غير صحيحة لغرض غير مشروع.

9) قدم بيانات غير صحيحة عن هويته أو تفويضه لمقدم خدمات التصديق بغرض طلب إصدار أو إلغاء أو تعليق شهادة.

10) قام عمدًا ـ بغير سند قانوني ـ بكشف بيانات سرية تمكن من الوصول إليها بما له من سلطات بموجب هذا القانون أو أي قانون آخر.

11) مارس نشاط مقدم خدمات تصديق بدون ترخيص.

12) استعمل بصفة غير مشروعة أداة إنشاء توقيع متعلقة بتوقيع شخص آخر.

13) قام بالدخول غير المشروع إلى حاسب آلي بقصد ارتكاب جريمة أو تسهيل ارتكاب جريمة سواء بواسطته أو بواسطة شخص آخر.

14) زور سجلا إلكترونيًا أو توقيعًا إلكترونيًا أو استعمل أيًا من ذلك مع علمه بتزويره.

15) قام عمدًا بطريقة غير مشروعة بنشر أو تسهيل نشر أو استعمال سجل إلكتروني أو توقيع إلكتروني أو فض شفرته، وتضاعف العقوبة إذا كان مرتكب الجريمة أمينًا على ذلك السجل أو التوقيع بمقتضى مهنته أو وظيفته.

كما حمى التوقيع الإلكتروني بنص خاص وعاقب:

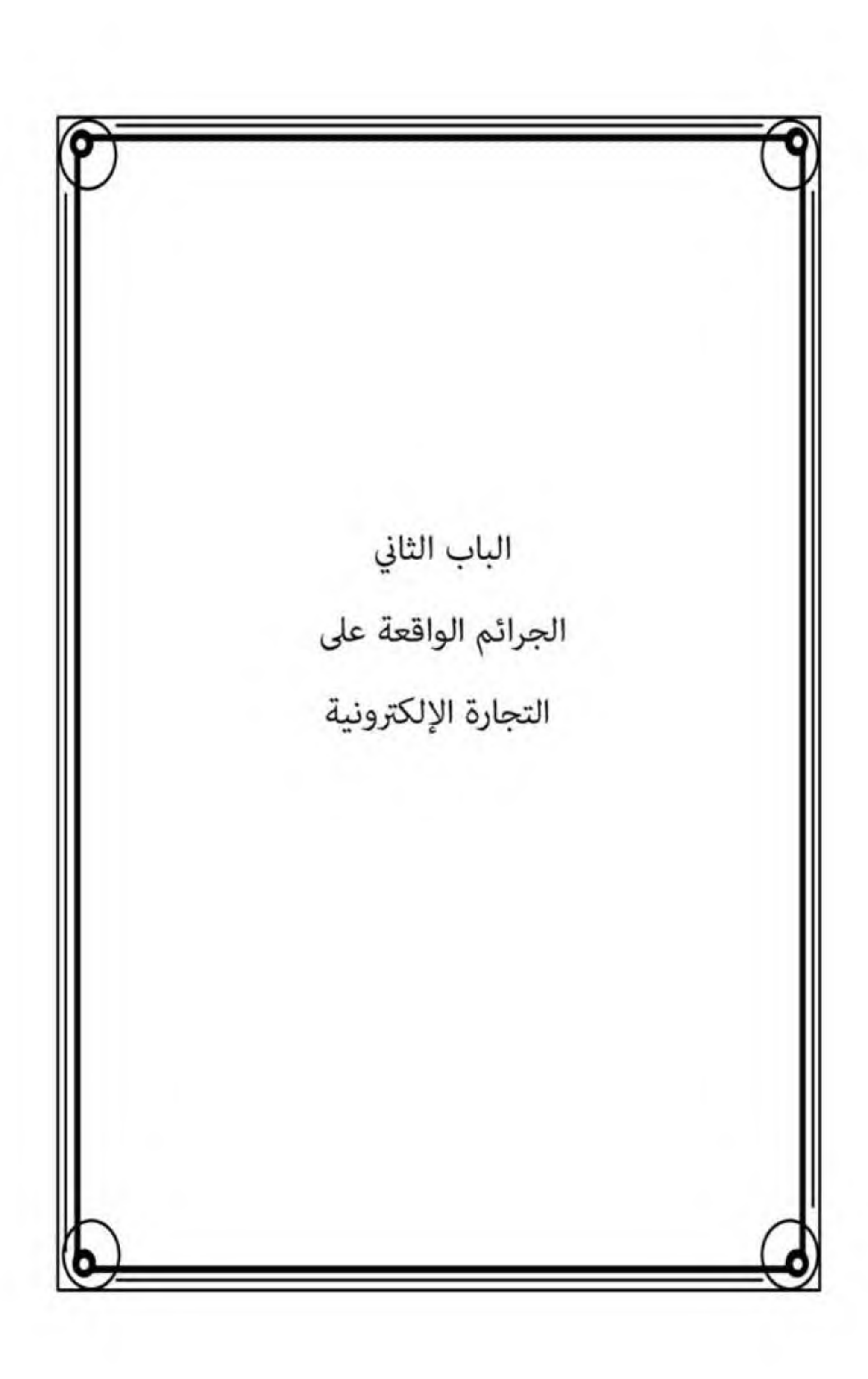
1) كل من صنع أو حاز أو حصل على نظام معلومات أو برنامج لإنشاء

توقيع إلكتروني دون موافقة صاحب ذلك التوقيع صراحة.

2) كل صاحب مفتاح تشفير رفض تسليمه للموظف الذى تحدده السلطة المختصة بعد الإفصاح عن هويته.

3) كل مقدم خدمات تصديق أو أحد العاملين لديه رفض تقديم تسهيلات للسلطة المختصة أو لأي من موظفيها للقيام بالمراقبة أو الإشراف أو التفتيش على أي نظام حاسب آلي أو جهاز بيانات أو مواد أخرى متصلة بنظام الحاسب الآلي بمقر مقدم خدمات التصديق.





الباب الثاني

الجرائم الواقعة على

التجارة الإلكترونية

الباب الثاني

الجرائم الواقعة على التجارة الإلكترونية

تمهيد وتقسيم:

يسرت التكنولوجيا وسهلت إنجاز المعاملات، وأتاحت فوق ذلك تقديم خدمات الرعاية بكافة نواحيها، كما أدت إلى تنمية الملكية الفكرية وكافة المجالات الأخرى، وعلى الرغم مما قدمته التكنولوجيا من خدمات وتسهيلات إلا أنها أضحت أداة فعالة ووسيلة مهمة لارتكاب الجرائم، فكانت هي ذاتها محلا للاعتداء الإجرامي، كما أنها على المستوى ذاته وبالدرجة ذاتها سهلت للمجرمين ارتكاب جرائمهم، وأدى ذلك إلى ظهور نوع جديد ومستحدث من الجرائم تعرف بجرائم شبكة الإنترنت وجرائم التجارة الإلكترونية، وانشغل فقهاء القانون الجنائي بشقيه الموضوعي والإجرائي بكيفية مواجهة هذا الوضع المستحدث[1]، وتباينت الحلول فذهب البعض إلى ضرورة إصدار قانون جنائي يعاقب على تلك الجرائم الإلكترونية، في حين ذهب آخرون إلى الاكتفاء بإدخال تعديلات على النصوص التشريعية الجنائية القائمة بطريقه تؤدي إلى استيعاب الصور المستحدثة من الجرائم الإلكترونية، في حين يرى فريق ثالث وعلى خلاف سابقيه أن النصوص القائمة في قانون العقوبات تكفي لاستيعاب هذه الصور المستحدثة من الجرائم الإلكترونية[2].

(1) Yacine Atif، A distributed and interoperable object،oriented support for safe e،commerce transactions، p 150، available at: www.elseviercomuterscience.com

(2) د. أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، ط 1، القاهرة، دار النهضة العربية، 2006، ص 4.

ومع تقديرنا لكافة الآراء التي قيلت في هذا الموضوع والتي سوف نتناولها بالقبول أو التعديل خلال دراستنا لبعض الجرائم المستحدثة في هذا الباب والذي نتناول فيه تحديدًا تلك الجرائم الواقعة على التجارة الإلكترونية عبر تقسيمه إلى فصول أربعة؛ يدور الفصل الأول حول الجرائم الواقعة على المواقع الإلكترونية، ويتكفل الثاني بدراسة الجرائم الواقعة على البيانات، ونتناول في الثالث الجرائم الواقعة على وسائل التجارة الإلكترونية، أما الفصل الرابع فإنه يتناول الجرائم الواقعة على الملكية الفكرية والحقوق المجاورة.



الفصل الأول

الجرائم الواقعة على المواقع الإلكترونية

تمهيد وتقسيم:

اهتمت كافة القوانين بحماية مواقع شبكة الإنترنت بصفه عامة، ومواقع التجارة الإلكترونية بصفة خاصة، وتأتي قوانين الولايات المتحدة الأمريكية وأوروبا في مقدمة هذه القوانين.

وتمثل الحماية الجنائية للتجارة الإلكترونية فرعًا من فروع الحماية القانونية لمواجهة الاعتداء على مواقع شبكة الإنترنت وصفحاتها، الذي يعد صورة من صور الاعتداء على النظم المعلوماتية بصفه عامة، ونظرًا لأن إعداد مواقع التجارة الإلكترونية يتطلب بالضرورة استخدام أجهزة كمبيوتر وبرامج مختلفة باعتبار أن نظام التجارة الإلكترونية كأي نظام معلوماتي يستند على قاعدة بيانات، وفوق ذلك يحتاج ويستند في نجاحه إلى ثقة كل الأطراف المتعاملين به، سواء أكانوا منتجين أم مستهلكين، وهو ما يقتضي دراسته حيث ندرس في المبحث الأول جريمة الدخول والبقاء والاعتراض غير المشروع على مواقع التجارة الإلكترونية، مع بيان ماهية الجريمة وأركانها، وفي المبحث الثاني ندرس جريمة إتلاف وتدمير مواقع التجارة الإلكترونية، وفي المبحث الثالث نتعرض لجريمة التزوير المعلوماتي، وفي المبحث الرابع نستعرض جريمة الاحتيال الإلكتروني.

المبحث الأول: جريمة الدخول والبقاء والاعتراض غير المشروع على مواقع التجارة الإلكترونية

المبحث الثاني: جريمة إتلاف وتدمير مواقع التجارة الإلكترونية

المبحث الثالث: جريمة التزوير المعلوماتي

المبحث الرابع: جريمة الاحتيال والنصب الإلكتروني

المبحث الأول

جريمة الدخول والبقاء والاعتراض غير المشروع على مواقع التجارة الإلكترونية

تشكل حماية المواقع والأنظمة المعلوماتية ومحتوياتها محور اهتمام الكثير من شركات المعلوماتية مع محاولة مجرمي شبكة الإنترنت العمل على توسيع الرقعة الجغرافية لعملياتهم، معتمدين في ذلك على عالمية شبكة الإنترنت، والتي تعطيهم القدرة للوصول إلى أصعب الأماكن بالرغم من جهود المؤسسات لمنعهم بمختلف أساليب الحماية التقنية.

والتقنية دائمًا لا تستطيع الصمود أمام ذكاء مجرمي شبكة الإنترنت أو ما يطلق عليهم مصطلح الهاكرز، وهم تلك الفئة من مجرمي شبكة الإنترنت الذين يمتازون بمهارة خاصة في التعامل مع التقنية لا يتمتع بها أقرانهم، ولا يستطيع الوقوف في طريقهم سوى القانون بصرامته وشدته، وسن التشريعات المناسبة التي تعاقب على أفعالهم الإجرامية.

ولقد أحدثت ثورة المعلومات والاتصالات تغييرات جذرية في المفاهيم القانونية على نطاق القانون الجنائي والمدني والتجاري، ومن أكثر المجالات التي تأثرت بهذا التطور المعاملات التجارية، فظهرت فكرة التجارة الإلكترونية عبر شبكة الإنترنت[1]، وكان لذلك أثره البالغ على التشريعات في الدول العربية، فنظمت بعض التشريعات العربية الموضوع، خصوصًا ما يتعلق بسبل الحماية الجنائية، ومن أهم هذه التشريعات قانون مكافحة جرائم تقنية المعلومات الاتحادي لدولة الإمارات العربية المتحدة رقم (2)

---

(1) **Steven Furnell، E.commerce security a question of trust، Computer fraud& security Magazine،p123.**

لسنة 2006، والذي يعد أول قانون عربي متخصص في هذا المجال, حيث جرم في مادته الثانية (كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام، أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحدى هاتين العقوبتين، فإذا كانت البيانات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن عشرة آلاف درهم، أو بإحدى هاتين العقوبتين).

وتعد جريمة الدخول غير المشروع للمواقع والأنظمة من أكثر الجرائم انتشارًا وارتباطًا بالتقنيات الحديثة وخصوصًا شبكة الإنترنت، وتقوم هذه الجريمة في الأساس على حب الفضول والاكتشاف بداية، ثم تقود إلى كثير من الجرائم الأخرى المرتبطة بها كالسرقة، والاحتيال، وإتلاف البيانات والمعلومات، وتزوير المستندات، وغيرها من الجرائم.[1]

(1) من أشهر القضايا في هذا المجال حادثة المواقع الإستراتيجية, ففي 19 تشرين الثاني 1999 تم إدانة Eric burns من قبل محكمة فيرجينيا الغربية بالحبس لمدة 15 شهرا والبقاء تحت المراقبة السلوكية لمدة 3 سنوات بعد أن اقر بذنبه وأنه قام وبشكل متعمد باختراق كمبيوترات محمية ألحق بها ضررا بالغا في كل من ولايات فيرجينيا وواشنطن إضافة إلى لندن في بريطانيا، وقد تضمن هجومه الاعتداء على مواقع لحلف الأطلسي، إضافة إلى الاعتداء على موقع نائب رئيس الولايات المتحدة، كما اعترف بأنه قد أطلع غيره من الهاكرز على الوسائل التي تساعدهم في اختراق كمبيوترات البيت الأبيض، وقد قام eric بتصميم برنامج أطلق عليه web bandit ليقوم بعملية تحديد الكمبيوترات المرتبطة بشبكة الإنترنت التي تتوفر فيها نقاط ضعف تساعد على اختراقها، وباستخدام هذا البرنامج اكتشف أن الخادم=

وتنص المادة 323-1 من قانون العقوبات الفرنسي الجديد على (الدخول أو البقاء بطريق الغش, داخل كل أو جزء من نظام المعالجة الآلية للمعطيات، يعاقب عليه بالحبس لمدة سنة وغرامة مقدارها 15.000 يورو, وإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المختزنة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها 30.000 يورو).

وسنتناول في هذا المبحث جريمة الدخول والبقاء غير المشروع لمواقع التجارة الإلكترونية، وفيه نبحث الركن المادي لكل من جريمة الدخول غير المشروع، وجريمة البقاء غير المصرح به في النظام، وجريمة الاعتراض غير المصرح به لنظام المواقع الإلكترونية، ونتبع ذلك بدراسة الركن

= الموجود في فيرجينيا والذي يستضيف مواقع حكومية وإستراتيجية منها موقع نائب الرئيس يتوفر فيه نقاط ضعف تمكن من الاختراق، فقام في الفترة ما بين آب 1998 وحتى كانون الثاني 1999 باختراق هذا النظام 4 مرات، وأثر نشاطه على العديد من المواقع الحكومية التي تعتمد على نظام وموقع USIA للمعلومات، وفي إحدى المرات تمكن من جعل آلاف الصفحات من المعلومات غير متوفرة، مما أدى إلى إغلاق هذا الموقع لثمانية أيام، كما قام بالهجوم على مواقع لثمانين مؤسسة أعمال يستضيفها خادم شبكة LASER.NET في منطقة فيرجينيا والعديد من مؤسسات الأعمال في واشنطن، إضافة إلى جامعة واشنطن والمجلس الأعلى للتعليم في فيرجينيا رتشموند، ومزود خدمات إنترنت في لندن، وكان عادة يستبدل صفحات المواقع بصفحات خاصة به تحت اسم ZYKLON أو باسم المرأة التي يحبها تحت اسم CRYSTAL.

- يونس عرب، جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10 - 12 /2/2002، ص 15.

المعنوي للجريمة في قصده العام وقصده الخاص، ثم نبين في نهاية هذا المبحث موقف التشريعات المختلفة من هذه الجريمة، وذلك وفقًا للتقسيم الآتي:

المطلب الأول: الركن المادي لجريمة الدخول والبقاء والاعتراض غير المشروع على مواقع التجارة الإلكترونية

المطلب الثاني: الركن المعنوي لجريمة الدخول والبقاء والاعتراض غير المشروع على مواقع التجارة الإلكترونية

المطلب الأول

الركن المادي لجريمة الدخول والبقاء والاعتراض غير المشروع لمواقع التجارة الإلكترونية

يتمثل الركن المادي في المظهر الذي تظهر به الجريمة إلى العالم الخارجي، ويقوم على عناصر ثلاثة، هي السلوك وهو ذلك النشاط الإيجابي أو النشاط السلبي الذي ينسب إلى الجاني، والنتيجة وهي الأثر الخارجي الذي يتمثل في الاعتداء على حق يحميه القانون، والسببية وهي الرابطة التي تصل بين السلوك والنتيجة، وعلى ذلك فإن هذه العناصر الثلاثة هي ماديات الجريمة[1].

وفعل الدخول غير المشروع للأنظمة والبرامج والشبكات، قد يكون مجرد دخول فقط، وقد يكون بقصد الوصول أو الحصول على بيانات ومعلومات، أو بقصد إلحاق الضرر بهذه البيانات أو بالأنظمة، كما قد يشكل البقاء بداخل النظام جريمة إذا كان هذا البقاء غير مشروع لكون الجاني

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، القاهرة، دار النهضة العربية، 1977، ص 51.

غير مصرح له أساسًا بدخول هذا النظام، أو أنه خالف الشروط والتعليمات وبقي في النظام بصورة غير مشروعة، كما يشكل اعتراض الوصول إلى الخدمة أو البرامج أو الأنظمة بأي صورة كانت جريمة أخرى.

وسنتناول في هذا المطلب من خلال أربعة فروع الركن المادي لكل من جريمة الدخول غير المصرح به، وجريمة البقاء داخل النظام، وجريمة الاعتراض غير المصرح به للنظام، فندرس الركن المادي لجريمة الدخول غير المصرح به في فرع أول، والركن المادي لجريمة البقاء غير المصرح به في فرع ثان، والفرع الثالث الركن المادي لجريمة الاعتراض غير المصرح به، وأخيرًا نتناول الدخول غير المصرح به ونظم حماية نظم الحاسبات الآلية، ومدى العلاقة بين تأمين هذه البرامج والأنشطة وحمايتها جنائيًا في فرع رابع.

الفرع الأول

الركن المادي لجريمة الدخول غير المصرح به

Illegal Access

يقصد بفعل الدخول هو ذلك الدخول إلى محتويات جهاز الكمبيوتر ذاته، أي إجراء اتصال بالنظام أو البرنامج محل الحماية بالطرق الفنية اللازمة لذلك.

وقد عرفه نظام مكافحة الجرائم المعلوماتية السعودي[1] بأنه: (دخول شخص بطريقة متعمدة إلى حاسب آلي، أو موقع إلكتروني أو نظام معلوماتي، أو شبكة حاسبات آلية غير مصرح لذلك الشخص بالدخول إليها).

(1) الصادر بالمرسوم الملكي السعودي رقم م/ 17 بتاريخ ٢٧ أبريل ٢٠٠٨.

ويرى الفقه الفرنسي أن الدخول لـه مـدلول معنـوي، حيـث إن الـدخول إلى نظـام معالجـة البيانات أو النظام المعلوماتي أو النظام الإلكتروني، يشبه الـدخول إلى ذاكـرة الإنسـان، كـما أن لـه مـدلولا ماديًـا يتمثـل في أن الشـخص يكـون قـد حـاول الـدخول أو دخـل بالفعـل إلى النظـام المعلوماتي.[1]

ولكي تقوم هذه الجريمة يجب ألا يكون النظام مفتوحًا أمام الجمهور، لأنه لو كان كذلك فلا جريمة؛ حيث يباح للجمهور الدخول والتجول في النظام، ولذلك فهذه الجريمة تفترض أنه لا يجوز دخول النظام سوى لأشخاص محددين.

ويتحقق فعل الدخول إلى النظام متـى دخـل الجـاني إلى النظـام كلـه أو جـزء منـه، وكـذلك يتحقق الدخول غير المشروع متى كان مسموحًا للجاني بالدخول لجزء معـين في النظـام وتجـاوزه إلى جزء آخر غير مسموح له بالدخول فيه.

كما يتحقق الدخول إلى الموقع أو النظام بالوصـول إلى المعلومـات والبيانـات المخزنـة داخـل نظـام الحاسـب الآلي بغـير حـق ودون تصريـح مـن المسـئول عـن هـذا النظـام أو المعلومـات لاستخدامها أو استغلالها، وأحيانًـا لمجـرد التسـلية وحـب الفضـول، أو لإثبـات التفـوق في الـنظم التكنولوجية وإثبات الذات.

ويفرق البعض بين نوعين من الدخول غير المشروع، الأول يعرف بدلالة المكان وهـو التسـلل في داخل النظام المعلوماتي، ويعرف الثاني من حيث الزمان ويتمثل في تجـاوز حـدود التصريـح أو الترخيص داخل النظام

(1) د. عبد الفتاح بيومي حجازي،جرائم الكمبيوتر والإنترنت في التشريعات العربية، مرجع سابق، ص 26.

والممنوح لفترة زمنية محددة عن طريق تجاوز هذه الفترة الزمنية.[1]

وفرق البعض الآخر في الدخول غير المصرح به إلى نظام الحاسب الآلي بين نوعين من السلوك:

1) العمليات التي تنطوي على اعتراض لعمليات الاتصالات من أجل الدخول إلى أحد أنظمة الحاسبات الآلية.

2) عمليات الدخول المباشر إلى هذه الأنظمة، وذلك بإحدى صور ثلاث للدخول غير المصرح به إلى أنظمة الحاسب الآلي ومواقع شبكة الإنترنت.

ففي الصورة الأولى يكون فيها الدخول إلى المعلومات في ذاتها، والثانية يتم الدخول إلى أنظمة الحاسب الآلي التي ترتبط فيما بينها من خلال شبكات الاتصال، والصورة الثالثة تتمثل في الدخول إلى شبكات المعلومات[2].

وقد يتمثل الفعل الذي يكوّن الركن المادي في الدخول المباشر إلى المعلومات أو النظام أو عملية الاعتراض غير المشروع، والقيام بعد ذلك بالإتلاف بداخل النظام، وفي كثير من الأحيان تقوم جريمة الدخول غير المصرح به بالفعلين معًا (الدخول والاعتراض).

فالدخول إلى المعلومات وأنظمة الحاسبات الآلية قد يتم بطريقة مباشرة عن طريق الحاسب الآلي الذي يحتوى على المعلومات والنظام، وقد يكون غير مباشر عندما يدخل الفاعل إلى هذه المعلومات والأنظمة بواسطة نظام آخر يتصل بالنظام الأول بواسطة شبكة الاتصالات، ويتم ذلك عن طريق

(1) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية،2000، ص 305.
(2) د. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، مرجع سابق، ص 28.

اعتراض النظام الأول.

ويتصل بالنوع الأول وهو الدخول المباشر، عمليات الدخول غير المصرح به التي تتم عن طريق الخارجين على هذه المؤسسات، وهم الموظفون الذين سبق لهم العمل في هذه الجهات ثم فصلوا منها لأي سبب كان، وإن كانت بعض هذه المؤسسات تستعين بهم لاحقًا للعمل كمستشارين في المجال المعلوماتي حتى تأمن مخاطرهم.

وتجدر الإشارة إلى أن الدخول غير المصرح به إلى شبكات المعلومات ليس من الضروري أن يكون دائمًا الهدف منه اعتراض اتصال للدخول إلى أنظمة الحسابات الآلية، فقد يكون الدخول بغرض الاستفادة من المزايا التي تقدمها الشبكة، دون دفع النفقات اللازمة لذلك.

ومجرد الدخول إلى نظام الحاسب الآلي لا تتحقق به الجريمة، وإنما يجب أن يكون هذا الدخول غير مشروع, أي أن الشخص الذي قام بالدخول لا يحق له الدخول كأن يكون لم يحصل على التصريح اللازم لذلك, أو لم تنطبق عليه الشروط اللازمة لذلك, أو أن صاحب النظام أو حائزه لا يسمح له بدخوله, أو أنه تجاوز الصلاحيات الممنوحة له.

ويرى جانب من الفقه أن الدخول في حالة مخالفة الشروط الخاصة بذلك, كأن يكون لم يقم بسداد مبلغ الاشتراك بالموقع, لا تقع به جريمة الدخول غير المشروع للنظام, على اعتبار أن الموقع مسموح بدخوله للجميع، وعدم التقيد بالشروط الموضوعة لا يرقى لمرتبة الدخول غير المشروع[1], ومع احترامنا لهذا الرأي إلا أنه يجب أن نفرق بين حالة سماح صاحب الموقع لهذا الشخص الذي قام بالدخول برغم عدم استيفائه للشروط,

(1) د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, مرجع سابق, ص 350.

وحالة الدخول دون رغبة صاحب الموقع أو النظام وذلك باتخاذ أساليب تقنية مكنته من الدخول رغمًا عن صاحب الموقع, ففي الحالة الأولى لا جريمة لرضاء صاحب الموقع, وفي الحالة الثانية نعتقد بوجود جريمة دخول غير مشروع للموقع أو النظام.

من ناحية أخرى فقد يتم اعتراض اتصال للدخول إلى المعلومات التي يقوم بنقلها دون الحاجة إلى الدخول في شبكة محلية، كما في حالة التقاط الإشارات التي يحدثها جهاز إلكتروني دون الحاجة إلى الدخول مباشرة داخل الشبكة التي تحمل الرسالة[1].

كما أن بعض التشريعات ذهبت إلى التفرقة بين جريمة الدخول غير المشروع، وجريمة الاعتراض والمتمثلة في إعاقة أو تعطيل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات.

والمعلومات الإلكترونية تشمل كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات، وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها.

أما البرنامج المعلوماتي فهو مجموعة من البيانات والتعليمات والأوامر قابلة للتنفيذ بوسائل تقنية المعلومات ومعدة لإنجاز مهمة ما.

ونظام المعلومات الإلكتروني يعد مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية أو غير ذلك.[2]

(1) د. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، 2004، ص 321.

(2) المادة (1) من القانون الاتحادي رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات لدولة الإمارات العربية المتحدة.

ويدور التساؤل حول الدخول غير المصرح به إلى النظام هل هو جريمة مادية يلـزم لتحققهـا أن يكون هذا الدخول منتجًا لأثره بمعنى أن يؤدي إلى تحقيق النتيجـة الإجراميـة وهـي الوصـول إلى المعلومات التي يحتوي عليها النظام أم جريمة شكلية؟ بمعنى أن الجريمة تتم بمجـرد الـدخول ولو لم يتم الوصول إلى النتيجة.

يلزم للإجابة على هذا التساؤل بيان المدلول المادي للنتيجة الإجرامية، سواء باعتبارها ظاهرة مادية أم ظاهرة قانونية.

النتيجة هي الأثر الخارجي الذي يتمثل في الاعتداء على حق يحميه القانون والذي يتضـمنه النص التشريعي، وتعد النتيجة في مدلولها القانوني عنصرًا في الـركن المـادي للجريمـة؛ لأن المشر ـع يجرم الاعتداء على الحق أو المصلحة الجديرة بالحماية، وبدون هـذا الاعتـداء لا يكـون للتجـريم محل، وإذا كان الأمر على هذا النحو فيما يتعلق بالنتيجة كفكـرة قانونيـة فـإن الأمـر يختلـف في خصوص النتيجة في مدلولها المادي، فإذا كانت النتيجة في هذا المدلول تبدو واضحة في كثـير مـن الجرائم إلا أن هناك عـددًا مـن الجـرائم تفتقـر فيـه النتيجـة لهـذا الوضـوح، كـالجرائم السـلبية البسيطة التي تقع بمجرد الامتناع دون أن يكون لهذا الامتناع أثر خارجي، كامتناع الأم عن إرضاع صغيرها[1]، وفي ضوء هذا التقسيم نجيب على ما بدأناه من تساؤل حول هل تعد جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي جريمة شكلية أم جريمة مادية؟

يـرى الـبعض أنـه مـن غـير الضرـوري أن يـنجح الفاعـل في الوصـول إلى النتيجـة الإجراميـة بالحصول على أي من المعلومات أو البرامج كي يتم النشاط الإجرامي في هذه الجريمة، بـل يكفـي مجرد الدخول إلى نظام

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، مرجع سابق، ص282.

الحاسب الآلي، حتى لو كانت العلة من تجريم الدخول غير المصرح به هي حماية المعلومات والبرامج من الوصول إليها والتلاعب بها، وتمثل هذه الجريمة عدوانًا محتملا على الحق، وليست من الجرائم التي تتمثل في تحقيق العدوان على الحق الذي يحميه القانون.

وتأخذ أغلب النصوص القانونية التي تناولت جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي في الدول المختلفة بالرأي المتقدم، حيث تسمح هذه النصوص بالعقاب على فعل الدخول غير المشروع إلى الأنظمة أو البرامج , دون الحصول على المعلومات أو البرامج, أو بمجرد أن يبدأ الفاعل بتشغيل الحاسب الآلي، في حالة الدخول المباشر إلى نظام الحاسب الآلي, فمنذ هذه اللحظة التي يبدأ الحاسب في العمل يتم إرسال إشارة كهربائية نحو وحدة المعالجة المركزية[1]، والتي تقوم بدورها بإرسال البرنامج المسئول عن تشغيل ذاكرة القراءة[2]، وتقوم هذه الذاكرة بالبحث عن المعطيات التي تسمح بتشغيل النظام المسئول عن البحث ثم تقوم بتسجيلها في ذاكرة القراءة والكتابة والتي تقوم بمتابعة المراحل اللاحقة، وحتى الآن لا يمكن القول بأنه قد تم الدخول فعليا إلى نظام الحاسب الآلي،

(1) وحدة المعالجة المركزية هي الوحدة المسئولة عن تنفيذ البرامج الموضوعة لها بدقة، وكذلك الإشراف على التوقيتات الموضوعة لهذه الأوامر، وكذلك الاتصال بالوحدات الأخرى، انظر: أيمن العشري، المرجع في أساسيات الحاسب الآلي للمبتدئين، 1997، ص 10.

(2) تقوم هذه الذاكرة بالقراءة فقط بينما لا تصلح للكتابة ولذلك فإن لها استخدامًا خاصا مع الحاسب الآلي، وهو تخزين البرامج الخاصة بتشغيل الجهاز فور فتحه، ويتم تشغيل هذه البرامج في كل مرة يتم فيها فتح الجهاز للعمل، انظر: المرجع السابق، ص 31.

وهو ما ذهبت إليه النصوص القانونية في كل من فرنسا [1]، التي اعتبرت أن الدخول المجرد يشكل الركن المادي لجريمة الدخول غير المشروع في صورتها اليسيرة (المادة 323-1)، وفي نفس الاتجاه سار المشرع الإماراتي (المادة 1/2).

وكذلك فإنه وفقًا للنصوص التي تتطلب أن يتم الدخول إلى معطيات يشملها النظام، كما هو الحال في النرويج والدانمرك والسويد فإنه يمكن القول بأن الدخول قد تم إلى المعطيات التي يشتمل عليها البرنامج المسئول عن تشغيل ذاكرة الحاسب، فوفقا لهذه القوانين فإن فعل الدخول قد انطوى على مساس بحق المسئول عن النظام في السيطرة عليه بغض النظر عن المساس بسرية المعلومات التي يحتوي عليها النظام.[2]

وتتباين التشريعات فيما بينها، ففي حين يسمح بعضها بتطبيق نصوص التجريم الخاصة بجريمة الدخول غير المصرح به إلى النظام بمجرد الدخول، نجد أن بعض التشريعات الأخرى تتطلب أن يتم الحصول على المعلومات التي يتضمنها النظام كشرط لقيام الجريمة، وتعد الولايات المتحدة الأمريكية مثالا على ذلك حيث تعاقب المادة 1030 (أ) (1) والمادة 1030 (أ) (2) من القانون الفيدرالي لجرائم الحاسب[3] على الدخول غير

(1) د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص333، 339.

(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998، ص 50.

(3) صدر هذا القانون عام 1984 وعدل أربع مرات في أعوام 1986-1994-1996، وأخيرا عام 2001 بمقتضى القانون الوطني The Patriot Act.

راجع حول ذلك د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 317.

المصرح به الذي يعقبه حصول على بعض المعلومات، أما المادة 1030 (أ) (3) من القانون ذاته فتعاقب على الدخول المجرد إلى الحاسبات الآلية داخل الحكومة الفيدرالية، أو الحاسبات التي لا تعمل داخل الحكومة الفيدرالية، بشرط أن يؤثر هذا الدخول على مصالح الحكومة التي ترتبط بشكل أو بآخر بهذه الحاسبات[1].

---

(1) (a) Whoever

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains،

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is

وإزاء هذا التباين بين التشريعات في تطبيق قواعد التجريم نجد أن المادة الأولى من قانون إساءة استخدام الحاسبات في إنجلترا قد جرمت الدخول باعتباره الفعل الذي يتم من خلال سلوك إيجابي يتمثل في أن يقوم الجاني بالدخول غير المشروع على الحاسب الآلي بأية طريقة كانت، أو الدخول للحصول على المعلومات، بمعنى أن يصل الفاعل إلى أي من المعلومات أو البرامج المخزنة داخل الحاسب، ولا يلزم أن تكون نية الفاعل متجهة إلى الوصول إلى معلومات أو برامج بعينها، بل إن تكون نية الفاعل متجهة إلى الوصول إلى معلومات أيًا كانت هذه المعلومات، فالغرض من هذا التجريم هو حماية المعلومات والبرامج من الوصول إليها، ويقصد بالمعلومات التي يجرم القانون الدخول غير المصرح إليها المعلومات بمعناها الواسع، وذلك نظرًا لكون الدخول إلى النظام يؤدي بالضرورة إلى الوصول إلى المعلومات المخزنة داخله، فإذا لم يتمكن مرتكب فعل الدخول من الوصول إلى المعلومات، وتم العدول عن إتمام المشروع الإجرامي فإن هذا العدول لا بد أن ينتج أثره، حيث لم تكتمل أركان الجريمة.

أما حماية النظام ذاته والحفاظ على حق المسئول عن النظام في السيطرة عليه فقد واجهته بعض التشريعات بالعقاب على الشروع في جريمة الدخول غير المصرح به، حيث إنه في هذه الحالة تم تجريم النشاط المتمثل في تشغيل الحاسب الآلي للدخول إلى النظام والمعلومات والبرامج التي يحتوي عليها، دون أن يتمكن الفاعل من الوصول إلى هذه المعلومات لأسباب خارجة عن إرادته[1].

---

exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص270.

وقد نصت بعض التشريعات صراحة على تجريم الشروع في جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، كما هو الحال في البرتغال والولايات المتحدة الأمريكية، حيث يعاقب على الشروع بذات العقوبات المقررة لجريمة الدخول غير المصرح به، وكذلك في فنلندا والسويد، حيث لا يعاقب على الشروع فقط بل كذلك على الأعمال التحضيرية التي تسبق هذه الجريمة[1].

هذا ويرى الجانب الأكبر من الفقه أن جريمة الدخول العمدي بغير وجه حق على موقع أو نظام معلوماتي من الجرائم الوقتية، وتقع من أي شخص يرتكبها، حيث يستوي أن يكون من الخبراء أو حتى من الأفراد العاديين، وسواء أكان الدخول للقيام بعمل غير مشروع أم لمجرد الفضول وحب الاستطلاع، ولا يشترط تحقق أي ضرر أو تلاعب في البيانات، وإنما تقع الجريمة بمجرد الدخول.[2]

وتعد كذلك من الجرائم الشكلية التي يكتمل شكلها القانوني بمجرد تحقق السلوك الإجرامي، دون تطلب عنصر آخر في الركن المادي للجريمة.

ويلزم الإشارة إلى أن القانون الإماراتي رقم 2006/2 في شأن مكافحة جرائم تقنية المعلومات نص في مادته (2) على أن: " كل فعل عمدي يتوصل فيه بغير وجه حق إلى موقع أو نظام معلوماتي سواء بدخول الموقع أو النظام، أو بتجاوز مدخل مصرح به، يعاقب عليه بالحبس وبالغرامة أو بإحدى هاتين العقوبتين، فإذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس

(1) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية تطبيقية، مرجع سابق، ص 357.

(2) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 51.

مدة لا تقل عـن سـتة أشـهر وبالغرامـة أو بإحـدى هـاتين العقـوبتين، فـإذا كانـت البيانـات أو المعلومات شخصية فتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التـي لا تقـل عـن عشرة آلاف درهم، أو بإحدى هاتين العقوبتين."[1]

وجاء في المادة (3): " كل من ارتكب أيًا من الجرائم المنصوص عليها في البند (2) مـن المـادة (2) من هذا القانون أثناء أو بسبب تأدية عمله أو سهل ذلك للغير، يعاقب بالحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن عشرين ألف درهم، أو بإحدى هاتين العقوبتين".

أما المادة (5) فنصت على أنه: " يعاقب بالسجن المؤقت أو الحبس كل مـن عـدل أو أتلـف الفحوصات الطبية، أو التشخيص الطبي، أو العلاج

(1) قبل صدور هذا القانون شهدت دولة الإمارات إحدى القضـايا في هـذا المجـال, حيـث تعتـبر هـذه القضـية واحدة من قضايا اختراق شركة الاتصالات التي تقدم خدمة شبكة الإنترنـت في الإمـارات، وتعـود وقائعهـا إلى 25 يونيو 2000 عندما تقدمت مؤسسة الاتصالات بشكوى لشرطة دبي تفيد أنها قامـت عـبر أجهزتهـا الخاصة بتسجيل اختراق لشبكة الإنترنت في الدولة عن طريق شركة عاملة في الدولـة وبواسـطة هواتفهـا، وبعد تحريات الشرطة تم التوصل إلى المتهم الذي يعمل لدى الشركة، والذي قام باختراق شبكة الإنترنت، وتسجيل بعض الملفات الخاصة بالمؤسسة وأسرار مستخدميها، واطلع على بعض الرسائل الخاصـة بـبعض المشتركين، وقد أحالته النيابة العامة للمحكمة بتهمة إساءة استخدام شبكة الإنترنت طبقـا للقـانون [1] لسنة 1991 في شأن مؤسسة الإمارات للاتصالات، وبالمادة [380] من قانون العقوبات الاتحادي بتهمـة فض رسائل دون إذن من أرسلت إليهم، وقد أدانته المحكمة عن التهمة الأولى، وعاقبته بالغرامـة عشرة آلاف درهم، وبرأته مـن التهمـة الثانيـة معتـبرة أن كلمـة الرسـائل الـواردة في المـادة لا تشـمل الرسـائل الإلكترونية، على اعتبار أنها استحدثت بعد صدور القـانون، إلا أن محكمـة الاسـتئناف قضـت في 6/ 10/ 2001 بإلغاء الحكم المستأنف، وتغريم المتهم عشرة آلاف درهم عن التهمتين، وأيـدت محكمـة التمييـز هذا الحكم في 8/ 12/ 2001. (القضية رقم 2000/5883 جنح دبي حكمت في 2001/7/10).

الطبي، أو الرعاية الطبية، أو سهل للغير فعل ذلك، أو مكنه منه، باستعمال الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات".

والملاحظ على هذه النصوص أن المشرع عاقب على كل فعل عمدي، واستثنى الدخول غير العمدي، وهنا يثار تساؤل حول ما إن كان الدخول إلى الموقع أو النظام مشروعًا أو صدفة أو عن طريق الخطأ، أو تجاوز الوقت المخصص لبقائه، وهنا أمام الفاعل أحد خيارين: إما الانسحاب سريعًا والخروج من الموقع، أو البقاء بصورة غير مشروعة في هذا الموقع، ونحن نرى أن المادة هنا لا تعاقب على البقاء في النظام بصورة غير مشروعة لكون نص المادة يعاقب على الدخول العمدي وما يترتب على هذا الدخول من أفعال ذكرت في الفقرة الثانية من هذه المادة، وليس بينها البقاء بصورة غير مشروعة في النظام أو الموقع، وإن كان هناك رأي في الفقه يرى أن الدخول بطريق الصدفة أو الخطأ أو السهو يتسم بعدم المشروعية، ويطرح تساؤلا حول تعدد الجرائم في حالة الدخول والبقاء غير المشروعين، ويؤكد أننا سنكون في هذه الحالة أمام جريمة واحدة؛ نظرًا لأن الجاني أراد بالدخول البقاء داخل النظام.[1]

كما أن المشرع نص على أن الدخول غير المشروع يأخذ إحدى صورتين وهما: دخول الموقع أو النظام، أو تجاوز مدخل مصرح به، ففي الصورة الأولى يكون الدخول بداية بصورة غير مشروعة، أما الصورة الثانية فيتصور أن يكون فعل الدخول هنا مشروعًا إلا أن الجاني تجاوز حدوده من هذا الدخول.

وشدد القانون في الفقرة الثانية من هذه المادة من عقوبة الجريمة إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 52.

إعادة نشر بيانات أو معلومات، كما شدد المشرع العقوبة في هذه الصورة إذا تمت الجريمة أثناء أو بسبب تأدية الجاني لعمله أو سهل ذلك للغير، ويستوي هنا العمل سواء أكـان خاصًّا أم عامًّا وفي ذلك حماية للوظيفة بالدرجة الأولى فضلا عن المعلومات أو البيانات التي قد يتحصل عليها الموظف بحكم وظيفته.

كما شدد العقوبة في الفقرة الثالثة من هذه المادة إذا كانت البيانات أو المعلومات شخصية، وفي ذلك حماية لبيانات الأشخاص الشخصية ومعلوماتهم الموجودة بداخل الأنظمة المتصلة بشبكة الإنترنت.

وإن كنا نتمنى أن تكون حماية البيانات والمعلومات الشخصية بصورة أعم تشمل أي جهة تقوم بجمع المعلومات والبيانات عن الأفراد والمؤسسات عبر الشبكة المعلوماتية وباستخدام وسائل تقنية المعلومات، وترتب عليها عقوبات في حالة قيامها بإفشاء هذه البيانات أو المعلومات دون إذن من صاحبها، ودون مقتضيات المصلحة العامة، ومن غير الحصول على أمر قضائي، كما أنه يجب معاقبة الجهات القائمة على تخزين هذه المعلومات والبيانات إذا ما قصرت في أخذ الاحتياطيات اللازمة لضمان أمن وخصوصية هذه المعلومات، أو إذا انحرفت عن الغرض أو الغاية التي من أجلها تم جمع هذه المعلومات والبيانات.

ولما تتصف به المعلومات والبيانات الحكومية من أهمية وسرية خاصة أفرد المشرع لها نصًّا خاصًّا في المادة (22) عندما عاقب بالسجن كل من دخل وبغير وجه حق موقعًا أو نظامًا مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات بقصد الحصول على بيانات أو معلومات حكومية سرية - إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك - فإذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو

تدميرها أو نشرها تكون العقوبة السجن مدة لا تقل عن خمس سنوات، ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

ففي هذه المادة اشترط المشرع أن يكون الدخول بقصد الحصول على بيانات أو معلومات حكومية سرية، ولكن لو تم الدخول بدون هذا القصد وتحصل الفاعل على بيانات حكومية سرية، ثم قام بنشرها أو احتفظ بها، فلا تنطبق عليه هذه المادة، ولكن يكون الانطباق للمادة الثانية من القانون.

ولأهمية المعلومات والبيانات الاقتصادية أيضًا فقد نصت المادة على سريان حكمها على المنشآت المالية كالبنوك والمنشآت المالية الأخرى وهي في اعتقادنا محلات الصرافة وما شاكلها، ولم يوضح المشرع هنا سر هذه التفرقة بينهما، بالإضافة إلى المنشآت التجارية والاقتصادية، وهنا يسري الحكم على هذه المنشآت سواء أكانت حكومية أو خاصة, ونعتقد أن هذه المادة أضفت مزيدًا من الحماية الجنائية الخاصة للتجارة الإلكترونية إذا ما كان قصد الجاني من الدخول الحصول على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

كما أن المشرع أفرد للمواقع الإلكترونية نصًا خاصًا في المادة (14) عاقب فيه بالحبس أو بالغرامة أو بإحدى هاتين العقوبتين كل من دخل بدون وجه حق موقعًا في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه.

وتختلف هذه المادة عن المادة الثانية في أن قصد الجاني من الدخول إلى الموقع هنا هو تغيير تصاميم هذا الموقع أو إلغاؤه أو تعديله أو شغل عنوانه، وبالتالي تقوم الجريمة ولو كان قصد الجاني تعديل هذا الموقع إلى الأفضل على اعتبار أن الموقع من اختصاص صاحبه لا يحق للغير إجراء

أي تعديل عليه، سواء للأفضل أو للأسوأ بدون وجه حق، ويلاحظ أن إتلاف الموقع قد يكون كليًّا أو جزئيًّا.

ومن ناحية أخرى فإن شغل عنوان الموقع يطلق عليه فعل التعطيل أو التعييب حيث يقوم بشغل العنوان، بحيث يبدو ظاهرًا لأي مستخدم يريد الدخول أن الموقع مشغول من كثرة الزائرين على حين أن الحقيقة هي أن الموقع مشغول وهميًّا بهدف حجبه عن الجمهور ومنعهم من الوصول إليه.

ويستوي في الأفعال السابقة أن يكون الجاني قد اقترفها عن طريق الشبكة المعلوماتية الدولية - أو عن طريق شبكة محلية - أو كان ذلك بوسيلة أخرى من وسائل تقنية المعلومات وهي كثيرة ومتعددة وقابلة للزيادة في المستقبل في ضوء ثورة المعلومات التي تشهدها البشرية في الوقت الحالي.

وجرم نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية[1] في مادته الثالثة عدة صور من ضمنها الدخول غير المشروع بالنص الآتي:

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة

(1) الصادر بالمرسوم الملكي السعودي رقم م/ 17 بتاريخ ٢٧ أبريل ٢٠٠٨, حيث صدر هذا النظام في ست عشرة مادة، تناولت المادة الأولى منها عشر فقرات أوضحت تعريفات المصطلحات والمسميات الواردة في النظام مثل "الشخص" و"النظام المعلوماتي" و"الشبكة المعلوماتية" و"البيانات" و"الجريمة المعلوماتية", كما حددت المادة الثانية أهداف النظام في الحد من هذه الجرائم والعقوبات المقررة لكل منها, وحددت مواد النظام الأخرى الجرائم المعلوماتية وعقوباتها التي تنوعت بين السجن لمدد مختلفة والغرامات المالية بحسب نوع وطبيعة كل جريمة من الجرائم المعلوماتية، وأوضحت المادتان الرابعة عشرة والخامسة عشرة اختصاصات كل من "هيئة الاتصالات وتقنية المعلومات" و"هيئة التحقيق والادعاء العام" في المساندة اللازمة للأجهزة الأمنية لتحقيق أهداف وغايات هذا النظام.

ألف ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1) التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي - دون مسوغ نظامي صحيح - أو التقاطه أو اعتراضه.

2) الدخول غير المشروع لتهديد شخص أو ابتزازه، لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا.

3) الدخول غير المشروع إلى موقع إلكتروني، أو الدخول إلى موقع إلكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.

4) المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا أو ما في حكمها.

5) التشهير بالآخرين، وإلحاق الضرر بهم، عبر وسائل تقنيات المعلومات المختلفة.

كما نصت المادة (5) من ذات النظام على أنه يعاقب بالسجن مدة لا تزيد على أربع سنوات وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين، كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

1) الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها أو تغييرها، أو إعادة نشرها.

2) إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها أو تدمير أو مسح البرامج، أو البيانات الموجودة أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها.

3) إعاقة الوصول إلى الخدمة، أو تشويشها، أو تعطيلها، بأي وسيلة كانت.

ومن القوانين العربية التي جرمت الدخول غير المشروع لنظام الحاسب الآلي قانون الجزاء في سلطنة عمان، حيث نصت المادة (276) مكرر على أنه: (يعاقب بالسجن مدة لا تقل عن 3 أشهر ولا تزيد عن سنتين وبغرامة 100 ريال إلى 500 ريال أو بإحدى هاتين العقوبتين كل من تعمد استخدام الحاسب الآلي في ارتكاب أحد الأفعال الآتية:

1) الالتقاط غير المشروع للمعلومات أو البيانات.

2) الدخول غير المشروع على أنظمة الحاسب الآلي.

3) التجسس والتصنت على البيانات والمعلومات.

4) انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم وتزوير بيانات أو وثائق مبرمجة أيا كان شكلها.

5) إتلاف وتغيير ومحو البيانات والمعلومات.

6) جمع المعلومات والبيانات وإعادة استخدامها.

7) تسريب المعلومات والبيانات.

8) التعدي على برامج الحاسب الآلي سواء بالتعديل أو الاصطناع.

9) نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكًا لقوانين حقوق الملكية والأسرار التجارية[1].

كما نص قانون المعاملات الإلكترونية العماني على معاقبة من قام بالدخول غير المشروع إلى حاسب آلي بقصد ارتكاب جريمة أو تسهيل ارتكاب جريمة سواء بواسطته أو بواسطة شخص آخر.

(1) المرسوم السلطاني رقم 2001/72 بتعديل بعض أحكام قانون الجزاء العماني، منشور في الجريدة الرسمية العدد (698) الصادرة بتاريخ 2001/7/1.

وعلى مستوى الدول الأوروبية جاءت الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست)[1] والصادرة في 23 نوفمبر 2001، بالنص في المادة (2) على تجريم الدخول غير المصرح به بالنص على أن: (تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الفعل التالي في قانونها الوطني، إذا ما ارتكب عمدًا وبغير وجه حق الدخول على كامل أو على جزء من منظومة كمبيوتر، ويجوز لطرف أن يستلزم أن ترتكب الجريمة عن طريق مخالفة التدابير الأمنية، بقصد الحصول على بيانات كمبيوتر أو بقصد آخر غير أمين، أو فيما يتعلق بمنظومة كمبيوتر أخرى).[2]

وجاء في المذكرة التفسيرية للاتفاقية[3] أن الدخول غير المشروع يشكل

(1) Convention on cybercrime، Budapest, 23.XI.2001

- وقعت على الاتفاقية الولايات المتحدة واليابان وكندا وجنوب إفريقيا إضافة إلى 26 دولة من أصل 43 من أعضاء مجلس أوروبا بينها 12 دولة من الاتحاد الأوروبي.
- www.cybercrime.gov/coedraft.html

(2) د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 2001) والبروتوكول الملحق بها، 2009، ص 12.

والنص الإنجليزي للاتفاقية كالآتي:

Article 2، Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system

(3) Draft explanatory Memorandum To the Draft Convention On Cybercrime Strasbourg 14 February 2001.

الجريمة الأساسية للتهديدات الخطرة والهجوم على أمن (مثل خصوصية ومصداقية وكينونة) نظم وبيانات الحاسوب، والحاجة إلى الحماية تعكس مصالح المنظمات والأفراد في إدارة وتشغيل والتحكم في تلك النظم دون إزعاج أو تحرج، فمجرد الاختراق غير المصرح به يجب من حيث المبدأ أن يكون غير مشروع بذاته، حيث إنه يمكن أن يقود إلى إعاقة المستخدم الشرعي للنظم والبيانات، ويمكن أن يتسبب في تعديل أو تدمير عالي التكلفة حال إعادة هيكلة كل ذلك.

مثل هذا الاختراق يمكن أن يتم على بيانات سرية (بما في ذلك كلمات العبور، والمعلومات حول النظم المستهدفة)، وكذلك إمكانية استخدام هذه النظم دون دفع، وارتكاب أشكال خطرة من الجرائم المرتبطة بالحاسوب، مثل الاحتيال، أو التزوير بطريق الحاسوب.

كما نصت المذكرة التفسيرية لهذه الاتفاقية على أن الدخول يتحقق بالوصول إلى كل أو جزء من نظام الحاسوب (القطع الصلبة، والملحقات، والبيانات المخزنة في النظام المعد، والأدلة وحركة البيانات ومضمونها المرتبط بهذه الحركة)، لذلك فهي لا تتضمن مجرد إرسال ملف أو مراسلة بريد إلكترونية إلى ذلك النظام.

كذلك فإن الدخول يشمل الوصول إلى نظام حاسوب آخر مرتبط بشبكة اتصالات عامة، أو إلى نظام حاسوب على ذات الشبكة، مثل LAN (شبكة منطقة محلية) أو الإنترانت من خلال منظمة ما، فمنهج الاتصال ليس بذي أهمية.

كذلك يجب أن يتم ارتكاب الفعل بدون وجه حق، أي أنه لا يوجد تجريم على الدخول من قبل المالك أو أي حائز شرعي للنظام أو لجزء منه، وأكثر من ذلك لا يوجد تجريم على الدخول إلى نظام حاسوب مسموح بالدخول

عليه مجانًا وبشكل مفتوح للعامة، فمثل هذا الدخول يعد دخولا بوجه حق.[1]

كما نص القانون العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات[2] وما في حكمها في المادة (3) على أن كل من دخل عمدًا وبغير وجه حق موقعًا أو نظامًا معلوماتيًا يعاقب بالحبس... والغرامة.... أو بإحدى هاتين العقوبتين.

فإذا كان الدخول بقصد إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو بإعادة نشر بيانات أو معلومات شخصية يكون الحد الأدنى لعقوبة الحبس... ولعقوبة الغرامة....

ومشروع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[3] نص في الفصل الثاني الخاص بالتجريم على أن تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقًا لتشريعاتها وأنظمتها الداخلية

(1) د. عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، بدون ناشر، 2005، ص 65.

(2) تم اعتماد " مشروع القانون العربي الاسترشادي لمكافحة جرائم المعلوماتية" بالقرار رقم (495) بتاريخ 2003/10/8م، الصادر عن الدورة التاسعة عشرة لمجلس وزراء العدل ومجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417 د 2004/21، بعد تعديل تسميته ليصبح " قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها"، والقانون متوفر على العنوان التالي:

http://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim_tech_info/loi_emir_ar_crim_tech_info.htm

(3) أعدت مشروع هذه الاتفاقية لجنة مشتركة من ممثلي مجلسي- وزراء العدل والداخلية العرب في تونس 2009, وجاء في المادة الأولى من الفصل الأول أن الهدف من الاتفاقية تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات, لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

(المادة الخامسة)، وبينت المادة السادسة جريمة الدخول غير المشروع بأنه:

1) الدخول أو البقاء، وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.

2) وتشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:

أ) محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة، وللأجهزة والأنظمة الإلكترونية وشبكات الاتصال، وإلحاق الضرر بالمستخدمين والمستفيدين.

ب) الحصول على معلومات حكومية سرية.

الفرع الثاني

الركن المادي لجريمة البقاء غير المصرح به

تتكون جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي من فعل الدخول الذي يتم عن طريق قيام الفاعل بإتيان كافة الأعمال الفنية اللازمة لإتمام هذا الدخول.

إلا أنه من ناحية أخرى قد يجد شخص نفسه داخل نظام لحاسب آلي غير مسموح له بالدخول إليه عن طريق الخطأ، كما لو كان في سبيله للدخول إلى نظام له الحق في الدخول إليه، ثم وجد نفسه بسبب خطأ ما كاستخدام شفرة خاطئة على سبيل المثال داخل نظام آخر، وفي هذه الحالة قد يقوم هذا الشخص بالخروج من هذا النظام بمجرد تبينه للخطأ الذي وقع فيه، وقد يستمر في البقاء داخل النظام على الرغم من معرفته أن هذا النظام غير مصرح له بالدخول إليه.

ولاشك أن البقاء داخل نظام الحاسب الآلي بعد دخوله عن طريق

الخطأ، لا يختلف عن الدخول غير المصرح به، من حيث كون الفعل في ظاهره غير مشروع، مما يتعين معه التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام، على الرغم من معرفته أنه غير مصرح له بالدخول إليه لا يختلف في جوهره عن الدخول غير المصرح به إلى نظام الحاسب الآلي، فالنتيجة الإجرامية في الحالتين واحدة، وهي الوصول إلى نظام غير مصرح بالدخول إليه، فالمصلحة التي يحميها القانون، وهي حماية نظام الحاسب الآلي، واحدة في الحالتين.

وقد اتجهت بعض التشريعات إلى النص صراحة على تجريم البقاء غير المصرح به داخل نظام الحاسب الآلي، ففي فرنسا تجرم المادة 323 - 1 صراحة الدخول أو البقاء غير المصرح بهما داخل كل أو جزء من نظام المعالجة الآلية للمعلومات، ولقد تم إدراج الجزء الخاص بالبقاء غير المصرح به إلى النص الفرنسي أثناء القراءة الأولى للقانون داخل مجلس الشيوخ الفرنسي على إثر التقرير الذي تقدم به أحد الأعضاء[1]، لصعوبة تطبيق النص في صياغته الأولى، والذي كان ينص فقط على الدخول غير المصرح به في حالة الدخول إلى النظام عن طريق الصدفة ثم البقاء داخل النظام على الرغم من عدم مشروعيته[2].

ولقد طبق القضاء الفرنسي المادة 323 - 1 في شأن حالة البقاء غير المصرح به داخل نظام الحاسب الآلي، حيث ذهبت محكمة استئناف باريس

(1) وقد تقدم بالاقتراح عضو مجلس الشيوخ الفرنسي "Thyraud" وأخذ به عند الصياغة النهائية للقانون.

(2) د. علي عبد القادر القهوجي، جرائم التعدي على نظام معالجة المعطيات، بحث مقدم لمؤتمر القانون الكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، مايو 2000، ص 50.

في حكم لها صادر في 5 أبريل 1994 إلى أن القانون يجرم البقاء غير المصرح به داخل نظام الحاسب الآلي[1]، سواء أكان الدخول قد تم عن طريق الخطأ، أو تم بطريقة مشروعة إلا أنه اكتسب بعد ذلك صفة عدم المشروعية، كما لو فقد الفاعل حقه في البقاء نتيجة لخطأ من جانبه.[2]

وفي الولايات المتحدة الأمريكية، وبعد التعديل الأخير للقانون الفيدرالي لجرائم الحاسب الآلي، تجرم المادة 1030/ أ/6 تجاوز الدخول المصرح به إلى نظام الحاسب الآلي، ولقد تم تعريف هذا التجاوز بأنه الدخول إلى حاسب آلي مع وجود تصريح بهذا الدخول، إلا أن الفاعل يستخدم هذا الدخول للحصول على معلومات أو لتعديلها دون أن يكون مصرحًا له بذلك، فالنص الأمريكي لا يتناول الحالات التي تنطوي على بقاء داخل النظام بعد دخوله على سبيل الخطأ، وإنما الحالات التي يكون فيها الدخول مصرحًا به ابتداءً، إلا أن القائم بهذا الدخول يتجاوز الحدود الممنوحة له ويبقي داخل النظام على الرغم من ذلك.

ويرى البعض أن البقاء غير المصرح به داخل نظام الحاسب الآلي لا يقتصر فقط على حالة الدخول إلى نظام غير مصرح بالدخول إليه على سبيل الخطأ والبقاء داخل النظام على الرغم من العلم بذلك، إنما ينطبق أيضًا على حالة الدخول إلى نظام الحاسب الآلي بموافقة المسئول عن النظام إذا كانت هذه الموافقة مشروطة بزمن محدد وحدث تجاوز لهذا الزمن، فإن

---

(1) Gabriel Roujou De Bauble، Bernard Bouloc، Jacques francillon، Yeves mayavd، CODE PENAL COMMENT،article par article، livres a 5، Dalloz، 1996 pp. 610.

(2) د. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، مرجع سابق، ص27.

البقاء داخل النظام في هذه الحالة يعد غير مصرح به.[1]

ويذهب البعض إلى أن الاختلاف بين جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، وجريمة البقاء داخل هذا النظام بعد دخوله عن طريق الخطأ يكمن في أن الأولى جريمة إيجابية من ناحية، ووقتية من ناحية أخرى، في حين أن الثانية جريمة سلبية من ناحية، ومستمرة من ناحية أخرى؛ لهذا لا يمكن الجمع بينهما في نص قانوني واحد نظرًا لاختلاف الطبيعة القانونية لكل منهما[2].

كما يرى فريق آخر أنه في حالة تجريم الدخول غير المصرح به إلى نظام الحاسب الآلي دون أن يشير النص إلى تجريم البقاء غير المصرح به، أو يتناوله بالتجريم نص آخر، فإن على القضاء أن يجيب عما إذا كان البقاء غير المصرح به داخل النظام يأخذ نفس الأحكام التي تسري على الدخول غير المصرح به أم لا.

يذهب هذا الرأي إلى أن الإجابة على هذا التساؤل تكمن في طبيعة جريمة الدخول غير المصرح به، فإذا كانت هذه الجريمة وقتية فإنها في بعض صورها تكون متتابعة الأفعال، حيث تقوم بأفعال متعددة يجمع بينها وحدة الحق المعتدى عليه ووحدة المشروع الإجرامي المستهدف بها، ويتحقق ذلك في حالة النصوص التي تجرم الدخول غير المصرح به والذي يستهدف الوصول إلى المعلومات أو البرامج، أو تلك التي تجرم الدخول إلى كل جزء من النظام، وذلك أنه بعد دخول الفاعل إلى النظام يمكن القول من

(1) د. أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، رسالة دكتوراه جامعة المنصورة، كلية الحقوق، 2006، ص 153.
(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 51.

الناحية التقنية أن فعل الدخول يتكرر بالدخول إلى كل معلومة وكل برنامج وكل جزء من النظام، بحيث تكون أمام أفعال متماثلة يعد كل منها جريمة في ذاته، لو اكتفى الجاني به لعوقب من أجله، وينتهي هذا الرأي إلى أنه في هذه الحالة يمكن العقاب على البقاء غير المصرح به؛ لأنه بعد اكتساب الدخول صفته غير المشروعة فإن الدخول يتحقق بالوصول إلى أية معلومة بعد ذلك أو أي برنامج، وجريمة الدخول غير المصرح يجب أن تنطوي على اختراق للإجراءات الأمنية الخاصة بالنظام، إذ يجب لاعتبار الجريمة متتابعة الأفعال في هذه الحالة أن تكون كل معلومة أو كل برنامج أو كل جزء من النظام تم الدخول إليه مشمولا بحماية هذه الإجراءات.

ويذهب أصحاب الرأي السابق إلى أنه في حالة النصوص التي تجرم مجرد الدخول غير المشروع إلى النظام فإنه لا يمكن العقاب على البقاء غير المصرح به ما لم ينص على ذلك صراحة كما هو الحال في القانون الفرنسي، إذ تقوم الجريمة بمجرد الدخول، فإذا كان هذا الدخول غير مصرح به ابتداءً فلا يمكن العقاب على البقاء داخل النظام ولو كان غير مصرح به ما لم ينص على ذلك صراحة[1] وفقًا لقاعدة الشرعية (لا جريمة ولا عقوبة إلا بنص)، وانحصار دور القضاء في تطبيق القانون وليس في سن التشريع، ووفقًا لقاعدة عدم القياس في التجريم.

وفي حكم لها صادر بتاريخ 5 أبريل 1999 ذهبت محكمة استئناف باريس إلى أن القانون يجرم البقاء غير المشروع داخل نظام الحاسب الآلي سواء أكان الدخول قد تم بطريق الخطأ، أو تم بطريقة مشروعة إلا أنه اكتسب بعد ذلك صفة عدم المشروعية كما لو فقد الفاعل صفة البقاء نتيجة

(1) د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص357.

لخطأ من جانبه[1].

والملاحظ أن قانون مكافحة جرائم تقنية المعلومات الإماراتي لم ينص على العقاب على جريمة البقاء غير المشروع كما ذهب القانون الفرنسي، وإنما نص في المادة الثانية على العقاب على من تجاوز مدخلا مصرحًا به، أي أنه من المفترض لقيام الجريمة هنا أن يكون الدخول مشروعًا وتجاوز نطاق هذا الدخول إلى منطقة افتراضية لا يجوز له الوصول إليها، ومثاله الموظف المختص بالعمل على جزء محدد من النظام ولا يسمح له بتجاوز هذا الجزء والدخول إلى أجزاء أخرى من النظام ليس من اختصاصه، فالموظف المختص بالعمل مع وكيل النيابة في التحقيق من صلاحياته الاطلاع على القضايا الخاصة بوكيل النيابة الذي يعمل معه، فإذا ما تجاوز حدوده وقام بالاطلاع فرضًا على القضايا الخاصة برئيس النيابة بأي طريقة كانت، عد مرتكبًا لجريمة تجاوز مدخل مصرح به المؤثمة قانونًا.

والمشرع الإماراتي هنا أغفل البقاء غير المصرح به بداخل النظام إن كان الدخول عن طريق الخطأ، رغم أنه عاقب على تجاوز المدخل المصرح بدخوله, وإن كنا نرى أنه إن بقي الجاني هنا بداخل النظام لفترة غير معقولة - تخضع في تقديرها لقاضي الموضوع - فإنه يعد مرتكبًا لجريمة دخول غير مشروع، على اعتبار أن المصلحة المحمية هنا هي هذا النظام غير المصرح بدخوله والوصول إليه، وكان يتعين على الفاعل هنا ضرورة مغادرة المكان الافتراضي الذي وجد نفسه فيه صدفة بأسرع طريقة ممكنة.

والجدير بالملاحظة هنا أنه من القوانين العربية التي عاقبت على فعل

(1) د. نائلة عادل, محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية تطبيقية، مرجع سابق، ص 358.

البقاء غير المشروع بداخل النظام القانون المغربي من خلال الفصل 607 - 3 في فقرته الثانية[1]، وقد سار في ذلك على نهج القانون الفرنسي عندما جرم البقاء غير المصرح به.

الفرع الثالث

الركن المادي لجريمة الاعتراض غير المصرح به

Illegal Interception

يتفق كل من الدخول غير المصرح به إلى نظام الحاسب الآلي والاعتراض غير المصرح به لهذا النظام في أن كلا منهما يؤدي إلى نتيجة واحدة، وهي الوصول إلى معطيات غير مصرح للفاعل بالوصول إليها، فالفاعل في الحالتين إنما أراد أن يصل إلى المعلومات المعالجة آليًا داخل هذا النظام، وهو يعلم أنه غير مصرح له بالوصول إليها، وقد يتم ذلك مباشرة عن طريق الدخول إلى نظام الحاسب الآلي، أو يتم بطريق غير مباشر عن طريق اعتراض الحاسب الآلي.

ويمكن تشبيه اعتراض نظام الحاسب الآلي بالتصنت على محادثة تليفونية على سبيل المثال، فهو يعني معرفة محتوى اتصال قد يتم داخل نظام حاسب آلي واحد، أو بين نظامين مختلفين، أو بين عدة نظم ترتبط فيما بينها من خلال شبكة اتصالات، وذلك بالتقاط المعلومات التي يتضمنها هذا الاتصال.

وتعد من وسائل اعتراض نظام الحاسب الآلي استخدام الموجات الكهربائية الصادرة عن الحاسب الآلي، فاعتراض نظام الحاسب الآلي كما هو معروف في الولايات المتحدة الأمريكية باسم التقاط الموجات الكهربائية

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 128.

هو جمع للمعلومات عن بعد، فمن الممكن جمع معلومات يتم إرسالها من خلال نظام الحاسب الآلي داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى وتقوم هذه الشاشة بالتقاط الموجات الكهربائية التي تحيط بالحاسب الآلي[1]، والتي تتحول إلى معلومات مقروءة على الشاشة من ناحية، كما يتم تسجيلها من ناحية أخرى.

ويختلف الدخول غير المصرح به إلى نظام الحاسب الآلي عن اعتراض هذا النظام من حيث النشاط الإجرامي في كل منهما، فالدخول إلى نظام الحاسب الآلي لا يتأتى إلا بتشغيل الحاسب للدخول إلى النظام بما يحتوي عليه من معطيات، أو الدخول عن بُعد باستخدام الشبكة العنكبوتية أو إحدى وسائل التقنيات الحديثة، أما في حالة التقاط المعلومات عن طريق اعتراض نظام الحاسب الآلي فإن عملية تشغيل الحاسب الآلي تكون قد بدأت بالفعل بواسطة شخص آخر غير الجاني، ويقتصر دور الفاعل هنا على اعتراضها للوصول إلى المعلومات التي تتضمنها عملية الاتصال.[2]

ولقد أدت هذه الاختلافات بين الدخول إلى نظام الحاسب الآلي وبين اعتراض هذا النظام إلى الاتجاه نحو إفراد نص خاص لتجريمه، وقد أوصى المجلس الأوروبي بضرورة إفراد نص خاص لاعتراض نظام الحاسب الآلي بمقتضاه يتم تجريم كل اعتراض لاتصال يتم من أو إلى أو

(1) د. نافذ ياسين، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص 413، تسمى هذه الموجات بالموجات الكهربائية التي تنبعث من الحاسب الآلي، ويمكن التقاطها من مسافة متر تقريبا أو أكثر في بعض الأحيان.

(2) د. حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007، ص325.

داخل نظام الحاسب الآلي أو شبكة للاتصالات[1].

وقد سار القانون البرتغالي على هذا النهج، حيث تجرم المادة الثامنة من القانون رقم 109 لعام 1991 الخاص بجرائم المعلوماتية اعتراض عمليات الاتصال التي تقوم على نقل المعلومات داخل نظم الحاسبات الآلية أو شبكات المعلومات باستخدام وسائل تقنية، بينما تجرم المادة السابعة الدخول غير المصرح به إلى نظم الحاسبات الآلية وشبكات المعلومات، وقد حددت المادة الثانية من هذا القانون المقصود بفعل الاعتراض، ووصفته بأنه كل عمل يهدف إلى الوصول إلى المعلومات التي تتضمنها نظم المعالجة الآلية للمعلومات باستخدام أجهزة كهرومغناطيسية أو سمعية أو ميكانيكية أو غير ذلك.[2]

ومن الجرائم الأخرى والمتعلقة بالإعتداء على شبكة الانترنت جريمة عرقلة الخدمة أو إعاقة الوصول إلى الشبكة، وحصول انقطاع في خدمة الاتصال بالشبكات أو بالخدمات التي تقدم إلى المستفيدين داخل الشبكة، من الجرائم المنتشرة على شبكة الإنترنت، وتتعدد الوسائل التي قد تتسبب في هذا الخطر، من ذلك إرسال حزم وهمية تملأ مساحات الذاكرة الوسيطة وتخرب معلومات تجزئة الرسائل، بحيث إذا حاول النظام المستقبل إعادة تركيبها عند الوصول فإن هذه المحاولة تتسبب في تخريب النظام[3].

---

(1) د. عطا عبد العاطي محمد السنباطي، موقف الشريعة الإسلامية من جرائم الحاسب الآلي، دراسة مقارنة، دار النهضة العربية،2002، ص37.

(2) د. نائلة عادل, محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية دراسة نظرية تطبيقية، مرجع سابق، ص 365.

(3) حسن طاهر داود، أمن شبكات المعلومات، مركز البحوث، معهد الإدارة العامة، الرياض، 2004, ص 103 وما بعدها. وراجع د. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت في التشريعات العربية، مرجع سابق، ص 140 وما بعدها.

والحقيقة أن الشبكات وما عليها من بيانات ومعلومات مخزنة عن طريق أجهزة حاسب آلي وتوصيلات وغيرها وبرامج محملة على هذه الأجهزة تتعرض للهجوم عليها من أشخاص شتى، يستوي أن تكون شبكة إنترنت، وشبكة إنترانت، وشبكة إكسترانت، وقد يتم ذلك عن طريق تقنيات الاتصالات الحديثة بواسطة الهواة الذين يستهدفون اللهو والتسلية دون قصد إلحاق الضرر بضحاياهم، وفي أغلب الأحوال فإن من اعتاد سلوك هؤلاء الأشخاص فإنه يتحول إلى فئة القراصنة[1]، وقد يتم بواسطة المخربين المحترفين، وهؤلاء الأشخاص مهمتهم الأساسية حال التجوال في فضاء شبكة الإنترنت هو التخريب، وهم يفعلون ذلك إما من باب الحقد على الآخرين أو لأن لهم مصلحة مادية في هذا العمل.

ومعظمهم هؤلاء يعمدون إلى التخريب المباشر والفوري قصير الأمد، أي الذي ينتج أثره فورًا، من ذلك قيامهم بمسح البيانات من جهاز الحاسب، أو تخريب التطبيقات على إحدى الشبكات، أو تعديل البرامج، أو تحريف البيانات، وتزوير المعاملات وغيرها من التصرفات التي تنقلهم إلى فئة مجرمي شبكة الإنترنت[2].

والحقيقة أن جريمة مهاجمة شبكات الاتصال يلجأ إليها المخترقون خاصة مهاجمة أنظمة الهاتف من منطلق التلصص فقط، وبالتالي أصبحت

(1) د. علي بن عبد الله عسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2004 , ص 45. وكذلك حسن طاهر داود، أمن شبكات المعلومات، مرجع سابق، ص 104.

(2) المرجع السابق، ص 106. وكذلك: د. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2007 , ص 76 وما بعدها.

خدمة الاتصالات معرضة للسرقة أو التصنت، والمجني عليه الذي يتحمل الأضرار الناجمة عن عمليات الاحتيال هو الجمهور[1]، وفي الوقت الحالي يمكن ممارسة هذه الأفعال غير المشروعة عن طريقة شبكة الإنترنت بهدف الحصول على الخدمات المتعلقة بالاتصالات بشكل غير قانوني دون الكشف عن الهوية، أو الاستيلاء على الخدمات المعلوماتية للقيام بأفعال غير مشروعة[2].

وتشمل سرقة وسائل الاتصالات الاستيلاء على الهواتف المحمولة، وتزوير بطاقة الهاتف، والوصول إلى لوحته لتحويل المكالمات، وهذه الجريمة هي من الجرائم الشائعة وقد يكون القصد منها عمل مكالمات لصالح المخترق، أو تضليل أجهزة العدالة لمنعهم من الوصول إلى المجرم الحقيقي[3]، وقد تمكن القراصنة من الدخول إلى هاتف المقر الرئيسي للبوليس البريطاني، وأجروا مكالمات هاتفية على حسابه بلغت مليون دولار أمريكي[4].

كما ساعدت نظم الاتصالات الحديثة - ومنها شبكة الإنترنت - عصابات الجريمة المنظمة وسهلت لهم عقد الصفقات غير المشروعة كالسلاح وغسيل الأموال، كما تستخدم تلك العصابات تقنيات التشفير الحديثة لنقل البيانات وتعزيز قدرتها بعيدًا عن رقابة الدولة، من أجل مباشرة

(1) د. عبد الفتاح بيومي حجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، 2003، ص 370.
(2) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، مرجع سابق، ص 134 وما بعدها.
(3) د. عبد الفتاح بيومي حجازي، الأحداث والإنترنت، مرجع سابق، ص 27.
(4) بيتر آن جرابسكي، الجريمة في فضاء شبكة الإنترنت، بحث منشور ضمن سلسلة الأمن والإنترنت، مركز بحوث شرطة دبي , ص 51.

أنشطتها الإجرامية[1].

والقانون الإماراتي الخاص بمكافحة جرائم تقنية المعلومات جرم في المادة (5) إعاقة أو تعطيل الوصول إلى الخدمة أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأي وسيلة كانت، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ويتضح من هذه المادة أن القانون رمى لحماية الخدمة أو الدخول إلى البرامج أو الأجهزة أو أي مصدر من مصادر البيانات أو المعلومات والتي تصل للمشتركين عن طريق مزود الخدمة، أو باستطاعتهم الوصول إليها، واستخدامهم لها بشكل سلس ومريح، فعاقب من يقوم بإعاقتهم للوصول إلى هذه الخدمة، أو دخولهم إلى الأجهزة أو البرامج أو مصادر البيانات، مهما كانت الوسيلة التي اتبعها الجاني في الإعاقة أو التعطيل، ومن شأن هذه الحماية المساهمة في تطور التقنية وانتشارها بشكل كبير.

والإعاقة أو التعطيل المنصوص عليهما في المادة لا يشترط في أي منهما أن يكون كليًا، فتعطيل الوصول إلى جزء من الخدمة أو شل حركتها جزئيًا، أو التسبب في ضعف أدائها، أو تعطيل وصول أشخاص معينين إليها، أو إلى الأجهزة أو البرامج أو مصادر البيانات ولو بشكل جزئي بسيط وبأي وسيلة تتحقق به الجريمة.

والسلوك الإجرامي في هذه الجريمة ينصرف إلى كل عمل من شأنه إرباك عمل نظام معالجة البيانات، ويستوي أن يكون من شأن نشاط الجاني إعاقة أو إفساد نظام التشغيل أو الإرسال، ويستوي أن يؤدي نشاط الجاني

(1) المرجع السابق، ص 53 . وراجع في تقنية التشفير د. عبد الفتاح بيومي حجازي، حجازي، الحكومة الإلكترونية ونظامها القانوني، المجلد الثاني، دار الفكر الجامعي، الإسكندرية، 2006، ص 100 وما بعدها.

إلى توقف النظام عن العمل بصورة دائمة أو مؤقتة، أو أن يستخدم الجاني في ارتكاب الجريمة أي وسيلة من شأنها أن تعوق حسن سير النظام كالاعتداء المادي على النظام أو نشر فيروس به، حيث يستوي لدى المشرع الوسيلة المستخدمة، ولا يشترط أن تكون الإعاقة بصورة كلية، بل يعاقب على هذا السلوك الإجرامي ولو أدى إلى إعاقة جزئية للنظام.[1]

وقد نصت اتفاقية بودابست الأوروبية في المادة (3) على تجريم الاعتراض غير القانوني بقولها: (يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية - وفقًا لقانونه الداخلي - واقعة الاعتراض العمدي وبدون حق، من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول وفي المنشأ أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات، كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية (بقصد الغش)، أو أن ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد بحاسب آخر.[2]

---

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 54.

(2) د.هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص59.

- والنص الإنجليزي للمادة كالآتي:

Article 3. Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non.public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

أما مشروع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فقد جرم في مادته السابعة الاعتراض غير المشروع، بنصه على تجريم الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية، وقطع بث أو استقبال بيانات تقنية المعلومات.

الفرع الرابع

الدخول غير المصرح به ونظم حماية نظم الحاسبات الآلية

تكفل الأنظمة الأمنية المختلفة الحماية لنظم الحاسبات الآلية في مواجهة الأخطار المختلفة سواء تلك التي تتمثل في الأخطار المادية الناشئة عن الكوارث المختلفة كالحرائق أو الزلازل، أو نقص أو زيادة التيار الكهربائي، أو تلك الناشئة بسبب الخطأ البشري، أو الأفعال الإجرامية المختلفة التي تتصل بالحاسبات الآلية، ويطلق على هذه القواعد نظم حماية الحاسبات الآلية.

وتندرج هذه القواعد تحت ما يطلق عليه قواعد الأمن المادي والتي تتمثل في حماية الحاسبات الآلية بوضعها في أماكن تكفل لها أن تكون بعيدة عن أية أعمال من شأنها تهديدها بأي شكل من الأشكال.

وتتميز بعض القواعد الأخرى بكونها أكثر تعقيدًا من قواعد الأمن المادي، ومن بينها وضع عوائق تحول دون التقاط الموجات الكهربائية المنبعثة من الأجهزة المختلفة، والتي يمكن عن طريقها معرفة محتوى المعلومات التي يتم نقلها، ويتأتى ذلك أيضًا عن طريق حماية الكابلات والوصلات الكهربائية لارتباطها بالأجهزة، ومن بين هذه القواعد أيضًا أسلوب يعتمد على توزيع العمليات التي يقوم بها نظام الحاسب الآلي، ونقلها إلى مركز المساعدة كنظام احتياطي عند الضرورة، ويلجأ إلى هذا الأسلوب

عادة البنوك وشركات التأمين، ويظل موقع هذا المركز سريًا ويخضع لدرجة عالية من الحماية، ومن الأساليب التي يتم اللجوء إليها أيضًا لحماية نظم الحاسبات الآلية من الدخول غير المصرح به إليها، الاعتماد على الاختبارات التقنية وذلك عن طريق التحقق من شخصية القائم بعملية الدخول، بواسطة البصمة الإلكترونية أو بصمة الصوت، ويتم اللجوء أيضًا إلى نظام التشفير لحماية المعلومات، ويقوم هذا النظام على تحويل المعلومات والبيانات إلى شكل رمزي غير مفهوم بدون مفتاح لحل رموزه يعرفه عادة مرسل المعلومات والمرسلة إليه، وفي داخل الحاسب الآلي ذاته توجد أجهزة مهمتها التحقق من شخصية القائم بعملية الدخول عن طريق شفرة الدخول.[1]

ويظل التساؤل حول مدى جدارة النظم المعلوماتية التي لا يوفر لها القواعد أو التدابير الأمنية الكفيلة بحمايتها جنائيًا ضد أفعال الدخول غير المصرح بها.

خلت أغلب القوانين من الإشارة إلى اختراق نظم حماية أنظمة الحاسبات الآلية، كشرط لتجريم الدخول غير المصرح به إلى نظام الحاسب الآلي، إلا أن ذلك لم يمنع من اختلاف الفقه حول هذا الموضوع، فمن ناحية ذهب فريق إلى القول بعدم جدارة النظم التي لا حماية تقنية لها، وقالوا: إنه من غير المقبول حماية معلومات مهمة تركها المسئولون عنها دون أية إجراءات تكفل لها الحماية، ويقيس أنصار هذا الاتجاه جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي على جريمة انتهاك حرمة مسكن

(1) Gabriel Roujou De Bauble، Bernard Bouloc، Jacques francillon، Yeves mayavd- CODE PENAL COMMENT،op cit 1996 pp. 220، 221.

الغير، بحيث لا تقوم الجريمة بمجرد الدخول إلى مسكن الغير، وإنما يجب أن يظهر ما يدل على عدم الرضا، أو أن يكون الدخول مصحوبًا باستعمال وسائل تدل على عدم رضا صاحب المسكن، كالتهديد أو الاحتيال.

وقد استند أنصار هذا الرأي إلى عدة أسباب ترجح في تقديرهم ضرورة أن يكون هناك نظم أمنية يتم اختراقها كشرط لامتداد الحماية الجنائية للمعلومات، ويتمثل السبب الأول في طبيعة نظم الحاسبات الآلية ذاتها، حيث إنه بانفتاح هذه النظم على الخارج، وذلك عبر شبكات المعلومات، وبالنظر إلى أهمية المعلومات التي تحتوي عليها في أغلب الأحوال، أصبح لزامًا على المسئولين عنها توفير الحماية اللازمة لها، وإلا أصبح الدخول إليها أمرًا ميسورًا، ويستند أنصار هذا الرأي إلى سبب آخر يتعلق بالمادة (28) من القانون الجنائي الفرنسي رقم 78 – 17 لعام 1978 الخاص بالمعلوماتية وحماية الحريات، حيث تتطلب أن تكون نظم المعلومات مشمولة بحماية تدابير أمنية، للحيلولة دون التلاعب بها أو إتلافها أو الدخول غير المصرح به إليها، والتي تحميها المادة 323 – 1 من قانون العقوبات.[1]

(1) ARTICLE 323.1

(Ordinance no. 2000.916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January2002)

(Act no. 2004.575 of 21 June 2004 article 45 I Official Journal of 22 June 2004)

Fraudulently accessing or remaining within all or part of an automated data processing system is punished by two

year's imprisonment and a fine of €30,000.

Where this behavior causes the suppression or modification of data contained in that system, or any alteration of

the functioning of that system, the sentence is three years' imprisonment and a fine of €45,000.

أما السبب الرئيسي في تقديرهم فيكمن في إقامة الدليل على قيام الركن المادي للجريمة، وفي التحقق من توافر القصد الجنائي لدى مرتكبها، حيث إن وجود مثل هذه النظم الأمنية واختراقها بواسطة الفاعل، يجعل من السهل التحقق من وقوع الجريمة، حيث يترك هذا الاختراق عادة أثرًا يدل عليه.

كما أن اختراق النظم الأمنية يعد وسيلة للتحقق من توافر القصد الجنائي ودليلا على وجوده.

وقد انتهى أنصار هذا الرأي إلى أن التفسير الصحيح للمادة 323 - 1 من قانون العقوبات الفرنسي، والخاصة بالدخول والبقاء غير المصرح بهما داخل نظام الحاسب الآلي، يقتضي لتجريم الدخول غير المصرح به أن يكون نظام الحاسب الآلي الذي تم الدخول إليه مشمولا بحماية النظم الأمنية، وأن يتم اختراق هذه النظم بالفعل، وذلك استنادًا إلى سببين:

الأول يتعلق بالأفعال التي تجرمها المادة سالفة الذكر، حيث تجرم الدخول غير المصرح به إلى نظام الحاسب الآلي من ناحية، والبقاء غير المصرح به داخل النظام من ناحية أخرى، وهما فعلان متميزان، فبينما يدخل الأول في عداد الجرائم الوقتية، يدخل الثاني في عداد الجرائم المستمرة، وهو ما يقتضي تمييزًا بينهما في الوسائل المستخدمة لارتكاب النشاط الإجرامي، ففي حالة الدخول غير المصرح به يتم النشاط الإجرامي عن طريق اختراق النظم الأمنية التي تحمي النظام، بينما لا تتطلب جريمة البقاء غير المصرح به داخل النظام مثل هذا الاختراق، إذ إنه من المفترض أن الدخول قد تم متوافقًا مع هذه النظم الأمنية.

أما السبب الثاني فيتمثل فيما تتطلبه المادة 323 - 1 من أن يكون فعل الدخول إلى نظام الحاسب الآلي قد تم عن طريق الغش والخداع، ويرى أنصار الاتجاه المتقدم أن هذا الوصف إنما يتصل بماديات الجريمة، وتفسير

ذلك أن فعل الدخول إلى نظام الحاسب الآلي تم عن طريق الغش والخداع، ومن ثـم كـان لزامًـا أن يتم تحديده بالإشارة إلى ضرورة أن يتم بيان وتحديد هذا الدخول أن يكون قد تم عن طريق الغش والاحتيال، وهو ما يتحقق في تقديرهم باختراق النظم الأمنية.

أما الاتجاه الثاني - والذي نؤيده - فهو يذهب إلى أنه ينبغي حماية نظم الحاسبات الآليـة والمعلومات التي تحتوي عليها، بغض النظر عن كونها تتمتع بحمايـة الـنظم الأمنيـة مـن عدمـه، ويقيس أنصار هذا الاتجاه جريمة الدخول غير المصرح به على جريمة السرقة، حيث إن تمتع المـال المسروق بحماية صاحبه أو عدم تمتعه بهذه الحماية لا يؤثر في قيام جريمة السرقة، فالجريمة قـد تمت بغض النظر عن مقدار الصعوبة التي واجهت الجاني في تنفيذها، كـما أن تطلـب مثـل هـذا الشرط من شأنه في كثير من الحالات أن يضيق على نحو كبـير مـن تطبيـق جريمـة الـدخول غـير المصرح به، ويجعل هذا التطبيق قاصرًا على الحالات التي تتمتع فيها الـنظم بالحمايـة، كـما أنـه يتجاهل الحالات التي يتم فيها الدخول إلى النظام نتيجة خطأ قام به المبرمجون أو المسئولون عن النظام.

أما فيما يتعلق بما تطلبته المادة 323-1 من أن يكون فعل الدخول إلى نظـام الحاسـب الآلي قد تم عن طريق الغش والاحتيال، فإن هذا الوصف إنما يتصل بـالركن المعنـوي للجريمـة، حيـث يشير إلى تطلب القصد العام لقيامها، ويستند أنصار هذا الاتجاه في تدعيم رأيهم إلى أنـه قـد تـم استبعاد شرط اختراق النظم الأمنية لتجريم الدخول غير المصرح به على الرغم من وجـود اقـتراح بإدراجه أثناء مناقشة القانون الخاص بجرائم المعلوماتية لعام 1988، والذي انتقلت نصوصـه إلى قانون العقوبات الجديد، وهو ما يدحض ما ذهب إليه أنصار الاتجاه الأول من أن المـادة 323-1 من قانون العقوبات

الفرنسي إنما تتطلب أن يتم الدخول إلى نظام الحاسب الآلي عن طريق اختراق النظم الأمنية، وقد أكدت محكمة استئناف باريس في حكم لها صادر عام 1994 على أنه من غير الضروري لقيام جريمة الدخول غير المصرح به[1]، أن يكون فعل الدخول قد تم بمخالفة للتدابير الأمنية، وأنه يكفي أن يكون هذا الدخول قد تم ضد إرادة المسئول عن النظام.

وقد تباين موقف التشريعات في الدول المختلفة أيضًا في الإجابة على هذا التساؤل، فقد استبعدت بعض التشريعات شرط اختراق النظم الأمنية لقيام جريمة الدخول غير المصرح به، ومنها على سبيل المثال كل من القانون الفرنسي- والمغربي والإماراتي والدنماركي والسويدي والإنجليزي والأسترالي والكندي[2].

أما التشريعات التي تطلبت لقيام جريمة الدخول غير المصرح به شروطًا تتعلق بالتدابير الأمنية، فنذكر منها على سبيل المثال: القانون النرويجي والفنلندي والهولندي والسويسري واليوناني والألماني، وقد اختلفت هذه التشريعات فيما بينها من حيث تحديد هذه الشروط، فتطلب بعضها أن يكون فعل الدخول نتيجة لمخالفة هذه التدابير الأمنية، كالقانون النرويجي والفنلندي والهولندي والسويسري.

واكتفت تشريعات أخرى بأن تكون المعطيات التي تم الدخول إليها

---

(1) henri des bois commerce electronique et proprieties' intellectuelles librairies techniques 2001 paris p127.

(2) انظر المادة 2 من قانون مكفحة جرائم تقنية المعلومات الإماراتي، والمادة 263 من قانون العقوبات الدانمركي، والمادة 21 من القانون السويدي للمعلوماتية لعام 1973، والمادة الأولى من القانون الإنجليزي الخاص بإساءة استخدام الحاسبات الآلية الصادر عام 1990، والفقرة الثانية والرابعة من المادة 76 من قانون العقوبات الأسترالي، والمادة 342 من قانون العقوبات الكندي.

مشمولة بحماية هذه التدابير الأمنية، بصرف النظر عن حدوث مخالفة فعلية لهذه التدابير، ومن الأمثلة على هذا الاتجاه القانون الألماني.

وقد حددت القوانين التي تطلبت مخالفة فعلية للقواعد الأمنية داخل الحاسبات الآلية الصورة التي قد تتخذها هذه المخالفة، فقانون العقوبات الفنلندي يعاقب على الدخول غير المصرح به إلى نظام الحاسب الآلي، متى كان الدخول قد تم عن طريق استخدام شفرة دخول غير مصرح باستخدامها، أو بالمخالفة لأية قاعدة أمنية أخرى، أما قانون العقوبات الهولندي فيعاقب على فعل الدخول متى كان نتيجة لمخالفة القواعد الأمنية الخاصة بالنظام، أو متى كان نتيجة لاستخدام أساليب تقنية كاستخدام شفرة غير صحيحة، ويعاقب قانون العقوبات النرويجي كل من يقوم بالدخول غير المصرح به إلى معطيات تم تخزينها أو يتم نقلها إلكترونيا عن طريق خرق الحماية التي تحيط بهذه المعطيات.

أما قانون العقوبات السويسري فيعاقب من يقوم بالدخول إلى نظام الحاسب الآلي مخترقًا لقواعد أمنية تحمي النظام، وقد انتقد الفقه النص السويسري بشدة، لما يمكن أن يؤدي إليه من نتائج تتعارض مع الغاية من تجريم الدخول غير المصرح به إلى نظم الحاسبات الآلية، فبمقتضى هذا النص فإن النظام الأمني التي تمت مخالفته يجب أن يكون موضوعًا بصفة خاصة في مواجهة الشخص الذي قام بالدخول غير المصرح به إلى النظام، وهو ما لا يتحقق في كثير من الحالات، وبصفة خاصة في الحالات التي يتم فيها الدخول عن طريق العاملين في المؤسسات المجني عليها، فالفاعل في هذه الحالة قد يقوم بالاستعانة بحاسب آلي متصل بشبكة الحاسبات الآلية داخل المؤسسة للدخول إلى نظام تمت إحاطته بقواعد أمنية في مواجهة حالات الدخول التي تتم من خارج المؤسسة، وهو ما يؤدي إلى عدم انطباق

النص على هذا الدخول.[1]

وقد اتجهت تشريعات أخرى إلى تجريم الأفعال التي تساعد على اختراق التدابير الأمنية داخل الحاسبات الآلية باعتبارها سلوكًا مجرمًا في ذاته، ففي الولايات المتحدة الأمريكية تعاقب المادة 1030 (أ) (6) من القانون الفيدرالي لجرائم الحاسبات الآلية على تبادل الشفرات الخاصة بالدخول إلى نظم الحاسبات الآلية، أو غير ذلك من المعلومات التي تساعد على الدخول غير المصرح به لنظام الحاسب الآلي، وفي كندا أيضًا يجرم القانون حيازة أو استعمال أو تبادل شفرة الدخول إلى الحاسب الآلي، والتي تسمح بالدخول غير المصرح به إليه[2].

المطلب الثاني

الركن المعنوي في جريمة الدخول والبقاء غير المشروع لمواقع التجارة الإلكترونية

يمثل الركن المعنوي الأصول النفسية لماديات الجريمة والسيطرة النفسية عليها، فهو في جوهره قوة نفسية، وهذه القوه هي الإرادة، ويتطلب القانون في الإرادة شروطًا كي يقوم بها الركن المعنوي، وهذه الشروط مجملها أن تكون الإرادة ذات أهمية قانونية، وتعد هذه الإرادة الإجرامية دليلا على خطورة شخصية الجاني، وتعد كذلك جوهر الركن المعنوي،

(1) المادة 202 من قانون العقوبات الألماني، المادة 370 من قانون العقوبات اليوناني، المادة 8 من الفصل 38 من قانون العقوبات الفنلندي، المادة 138 من قانون العقوبات الهولندي، المادة 145 من قانون العقوبات النرويجي، المادة 143 من قانون العقوبات السويسري.

(2) المادة 1030 (أ) من القانون الفيدرالي لإساءة استخدام الحاسبات الآلية في الولايات المتحدة الأمريكية، والمادة 342 من قانون العقوبات الكندي.

ويمثل الركن المعنوي للجريمة ركن المسئولية الجنائية، فإذا انتفى الركن المعنوي كنا بصدد مانع من موانع المسئولية الجنائية، ويفترض الركن المعنوي في الفاعل توافر الأهلية الجنائية، ويتطلب الركن المعنوي عنصرين: وجود إرادة معتبرة قانونًا، واتجاه هذه الإرادة على نحو مخالف للقانون.[1]

ويتخذ الركن المعنوي لجريمتي الدخول غير المصرح به إلى النظام والبقاء فيه صورة القصد الجنائي باعتبارهما من الجرائم العمدية[2]، وحتى يتوافر لهذه الجريمة ركنها المعنوي، يجب أن تتحقق عناصر القصد الجنائي من علم وإرادة، ويشكل الركن المعنوي[3] أهمية في قيام جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، فالأفعال التي تقوم بها هذه الجريمة يقوم بها كل يوم مستخدمو الحاسبات الآلية، ومن بين جميع هذه الأفعال لا يمكن تجريم سوى تلك التي يتحقق بشأنها القصد الجنائي، وسوف نتناول فيما يأتي القصد العام المطلوب تحققه في جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي (فرع أول)، ثم نتعرض لبعض التشريعات التي تطلبت قصدًا خاصًا في هذه الجريمة (فرع ثان).

(1) د. محمود نجيب حسني، شرح قانون العقوبات، مرجع سابق، ص 518، 522.
(2) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص171.
(3) د. حسام الأهواني، الحاسب الآلي والحياة الخاصة بحث منشور في مجلة العلوم والاقتصاد، كلية الحقوق، جامعة عين شمس، عدد يناير، 1990، ص164.

الفرع الأول

القصد العام في جريمة الدخول والبقاء غير المشروع لمواقع التجارة الإلكترونية

تقر جميع التشريعات الجنائية التي تناولت جريمة الدخول غير المصرح به إلى النظام بضرورة توافر القصد الجنائي العام بشقيه العلم والإرادة في هذه الجريمة، وإن كانت النصوص القانونية قد جاءت على اختلاف فيما بينها في العبارات المستخدمة لهذا الغرض، ففي الوقت الذي يعبر فيه النص الفرنسي عن القصد العام الذي يتطلبه فإنه يستلزم أن يكون الدخول إلى النظام قد تم عن طريق الغش والخداع، فاستخدام هذه العبارة يعني أن الفاعل على علم بأن دخوله إلى نظام الحاسب الآلي غير مصرح به.[1]

في حين أن النص في بعض التشريعات الأخرى كالولايات المتحدة الأمريكية وفنلندا وسويسرا والبرتغال يشير إلى أن الفاعل يقوم بالدخول غير المصرح به إلى النظام على نحو مخالف للقانون، بمعنى أنه يشترط أن يتم الدخول إلى النظام بدون تصريح، في حين أن النص في القانون السويدي واليوناني يشترط أن يتم الدخول إلى النظام على نحو غير مصرح به مع العلم بذلك، وفي أستراليا يلزم أن يتم الدخول عمدًا وعلى نحو غير مشروع أو بدون وجه حق[2].

وفي كل الأحوال وفي كافة النصوص الجنائية يتطلب القصد العام أن يحيط علم الجاني بكل واقعة ذات أهمية قانونية في تكوين الجريمة، فكل ما

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 174.

(2) د. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، مرجع سابق، ص379.

يتطلبه القانون من وقائع لبناء أركان الجريمة واستكمال عناصرها يتعين أن يشمله علم الجاني، ولكن علم الجاني لا يقتصر نطاقه على الوقائع التي تدخل في تكوين الجريمة، وإنما يتعين أن يحيط أيضًا بالتكييف الذي تتصف به بعض هذه الوقائع وتكتسب به أهميتها في نظر القانون، حيث إن عددًا من الوقائع التي تقوم بها الجريمة لا تمثل أهمية في نظر القانون إلا إذا اكتسبت وصفًا معينًا، فإن تجردت من هذا الوصف فقد تجردت من الأهمية القانونية ولم تعد صالحة لتقوم بها الجريمة[1].

ونخلص من هذه المبادئ العامة إلى أنه في الدخول غير المصرح به إلى النظام، ينبغي أن يحيط الجاني علمًا بكل واقعة ذات أهمية قانونية تدخل في تكوين هذه الجريمة، كأن يحيط علم الجاني بالركن المادي للجريمة، والذي يتضمن موضوع الحق المعتدى عليه، أي أن يعلم الجاني أن فعله ينصب على نظام الحاسب الآلي بما يتضمنه من معلومات وبرامج، باعتباره محل الحق الذي يحميه المشرع، فإذا اعتقد الفاعل بناءً على أسباب معقولة أنه يقوم بإجراء بعض العمليات عن طريق الحاسب الآلي، دون أن يتجه علمه إلى أنه يقوم بالدخول إلى نظام الحاسب بما يحتوي عليه من معلومات وبيانات، فإن القصد الجنائي العام في جريمة الدخول لا يتوافر لديه، وعلى الرغم من الأهمية القانونية لذلك إلا أنه من الناحية العملية يفقد هذه الأهمية لأنه نادرًا ما يدخل الفاعل إلى نظام الحاسب الآلي وهو غير عالم بذلك، نظرًا للخبرة التي يتمتع بها المجرم المعلوماتي في أغلب الأحوال والتي تمنع التسليم بهذا الفرض، ومع ذلك فإنه إذا ثبت انتفاء هذا العلم انتفى القصد الجنائي بدوره.

---

(1) د. محمود نجيب حسني، النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، 1988، ص 51.

وإلى جانب علم الجاني بموضوع الحق الذي يناله الاعتداء بارتكاب الجريمة، فإنه يتعين أن يعلم أيضًا بخطورة الفعل الذي يقوم به على الحق الذي يحميه القانون، وبناءً على ذلك إذا كان الدخول إلى نظام الحاسب الآلي قد تم عن غير علم بخطورة الفعل على الحق الذي يحميه القانون، فإن القصد الجنائي يعد منتفيًا.

ويثار التساؤل حول ما إذا كان دخول الفاعل الذي يعمل في مجال المعلوماتية ولم يصرح له بالدخول إلى النظام قد تم بهدف منع خطر ما يهدد النظام، فهل يترتب على هذه المحاولة ارتكاب الفعل المجرم بالدخول إلى نظام غير مصرح له بالدخول إليه، أم أن ذلك يعد انتفاءً للعلم، إذ إنه أتى الفعل وهو يعتقد أنه لا مساس له بالحق الذي يحميه القانون، وبالتالي لا يعد القصد الجنائي متوافرًا في هذه المرحلة، أم أن محاولة منع هذا الخطر يعد باعثًا على ارتكاب الفعل، وهو ما لا ينفي القصد الجنائي.[1]

ويتطلب القصد الجنائي أيضًا أن يتوقع الجاني حين يأتي فعله النتيجة الإجرامية التي سوف تترتب على الفعل، ويمثل توقع النتيجة الأساس النفسي الذي تقوم عليه إرادته[2]، والنتيجة التي يجب أن يتوقعها الجاني هي النتيجة بعناصرها التي يحددها القانون وفي النطاق الذي يرسمه لها، فلا يشترط أن يتجه التوقع إلى عناصر أو حدود أو آثار لا يدخلها المشرع في فكرة النتيجة ولو كان من شأنها أن تعطيها مزيدًا من التحديد، وهي في هذا المقام الدخول غير المصرح به إلى النظام، لذا لا يلزم أن يتجه التوقع إلى الآثار غير المباشرة التي لا يدخلها القانون في تحديد النتيجة، فالقصد

(1) د. أحمد عوض بلال، شرح قانون العقوبات، القسم العام، دار النهضة العربية، 2007، ص 590.
(2) د. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، مرجع سابق، ص610.

الجنائي يتوافر ولو لم يتوقع الجاني هذه الآثار، فيتعين إذًا أن يتوقع الجاني أنه سوف يدخل إلى نظام غير مصرح له بالدخول إليه، ولا يشترط أن يتوقع الضرر الذي سوف يلحق النظام أو صاحبه من جراء هذا الدخول.

والنتيجة التي يجب أن يتوقعها الجاني هي النتيجة بعناصرها التي يحددها القانون فلا يشترط أن يتوقع الجاني عناصر لا يدخلها المشرع في فكرة النتيجة، فيكفي أن يتوقع الجاني الدخول إلى نظام الحاسب الآلي غير المصرح له بالدخول إليه، ولا يشترط أن يتوقع الدخول إلى نظام بعينه، وهو ما يحدث من الناحية العملية في كثير من الحالات، فإذا توقع الفاعل أنه بصدد الدخول إلى نظام معين، ثم يترتب على فعله الدخول إلى نظام آخر، فإن القصد الجنائي يظل متوافرًا لديه، فالأصل العام حتى تتحقق النتيجة الإجرامية أن المادة (17) من قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة[1] قد نصت على أن التحقق من توافر النية الإجرامية

---

(1) (1) The following provisions of this section apply for the interpretation of this Act. 17.
(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he،
(a) alters or erases the program or data;
(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;
(c) uses it; or
(d) has it output from the computer in which it is held (whether by having it displayed or in any other manner);and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.
(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform،
(a) causes the program to be executed; or
(b) is itself a function of the program. =

في جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي، لا ينبغي أن

= (4) For the purposes of subsection (2)(d) above،

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) Access of any kind by any person to any program or data held in a computer is unauthorized if،

(a) he is not himself entitled to control access to the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7) A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer،

(a) any program or data held in the computer concerned is altered or erased; or

(b) any program or data is added to its contents; and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Such a modification is unauthorised if،

(a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

(b) he does not have consent to the modification from any person who is so entitled.

(9) References to the home country concerned shall be read in accordance with section 4(6) above.

(10) References to a program include references to part of a program.

ترتبط بنوعية المعلومات أو البرامج أو النظم محل الجريمة، فالفاعل يسأل عن جريمته ولو لم يكن دخوله مصحوبًا بتحديد المعلومات أو البرامج التي تم الدخول إليها.

وإذا كانت الوقائع السابقة، مما يتعين أن يحيط بها علم الجاني لما لها من أهمية قانونية في تكوين الجريمة، فإن هناك وقائع يسأل الجاني فيها عن الجريمة دون أن يتطلب القانون علمه بها، فمن ناحية لا يشترط أن ينصرف قصد الجاني إلى ما قد يترتب على فعل الدخول من إتلاف المعلومات أو إلحاق ضرر بصاحب هذه المعلومات بصفة عامة، ما لم يتطلب النص قصدًا خاصًا.

ويدور التساؤل هنا حول ماذا لو أن ما توقعه الجاني من نتيجة لم يحدث كاملا، وهل يعني الاختلاف انتفاء القصد أم أن هناك اختلافًا ينفيه وآخر لا يعتد به القانون؟ والإجابة أن علم الجاني يتعلق بالظروف المشددة التي تغير من وصف الجريمة[1]، فإذا كانت الظروف المشددة ترتبط بدرجة جسامة النتيجة المترتبة على فعل الجاني فإنه يلزم أن ينصرف علم الجاني إلى تلك الظروف حتى يمكن توقيع العقاب المشدد، لأنه حين يقرر القانون لبعض الجرائم عقابًا معينًا إذا أحدث الفعل نتيجة ذات جسامة معينة، فإذا ازدادت جسامة هذه النتيجة، فأفضت إلى نتيجة أشد جسامة شدد القانون العقاب، ولكنه لا يتطلب انصرافه إلى النتيجة الأشد جسامة بحيث يسأل الجاني عنها على الرغم من عدم توقعه لها.[2]

ومن ناحية أخرى لا يتعين انصراف قصد الجاني إلى الوقائع التي يقوم

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، مرجع سابق، ص 611.
(2) المرجع السابق، ص 611.

عليها التشديد إذا لم يغير من وصف الجريمة ولم يعدل أحد أركانها، وإنما اقتصر على مجرد تشديد العقاب، وبناءً على ذلك فإنه إذا شدد المشرع عقوبة الدخول غير المصرح به إلى نظام الحاسب الآلي في بعض الحالات، كما لو كان هذا الدخول قد تم عن طريق اختراق نظم الأمن الخاصة بنظام الحاسب الآلي، فإنه لا يجب أن يتصل علم الجاني إليها.

ولا تقتصر فكرة القصد الجنائي على العلم بالوقائع فقط، بل تتطلب العلم باكتساب بعض هذه الوقائع تكييفًا معينًا، فبعض الجرائم لا تقتصر عناصرها على وقائع مجردة عن التكييف، بل يعد التكييف الذي تكتسبه هذه الوقائع من بين عناصرها الأساسية، وفي مثل هذه الجرائم يمثل التكييف ذات الأهمية القانونية التي تمثلها الوقائع في ماديتها، ولما كان القصد الجنائي يتطلب علمًا بكل عناصر الجريمة، فهو يتطلب حتمًا انصراف العلم إلى التكييف، كما يتطلب إحاطته بالوقائع[1]، فإذا كان التكييف عنصرًا في الجريمة، إذ بدونه ينتفي أحد أركانها، وتصبح الواقعة التي تجردت من هذا التكييف غير ذات أهمية قانونية في تكوين الجريمة، فإنه ينبغي أن يشمل علم الجاني هذا التكييف كي يتوافر القصد الجنائي.

وتطبيقًا لذلك يتعين أن يعلم مرتكب جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي أن دخوله إلى هذا النظام غير مصرح به، فعدم وجود هذا التصريح هو تكييف لواقعة الدخول إلى نظام الحاسب الآلي يتعين العلم به، فإن انتفى هذا العلم اعتبر القصد الجنائي في هذه الجريمة غير متوافر.

وإذا ما توافر العلم على النحو السابق، تعين بعد ذلك القول بتوافر القصد الجنائي، بحيث تتجه إرادة الجاني نحو الدخول إلى النظام غير

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 176.

المصرح به بالدخول إليه، أي أن تتجه إرادته لتحقيق هذه النتيجة، ولا عبرة بعد ذلك بالباعث أو الغاية من وراء هذا الدخول، حيث إنهما لا يعدان من عناصر القصد الجنائي، وإن كانا نبيلين فهما لا ينفيانه، ويترتب على ذلك أن ادعاء الجاني بأن الغاية من دخوله إلى النظام غير المصرح له بالدخول إليه إنما تكمن في رغبته في الكشف عن أوجه القصور التي تعتري للنظام الذي تمكن من الدخول إليه، وذلك لتلافي هذا القصور مستقبلا، لا يحول ذلك دون القول باتجاه الإرادة لتحقيق النتيجة التي يجرمها المشرع، وهي الدخول إلى نظام غير مصرح بالدخول إليه.[1]

الفرع الثاني

القصد الخاص في جريمة الدخول والبقاء غير المشروع لمواقع التجارة الإلكترونية

يقوم القصد العام على العلم والإرادة المنصرفين إلى أركان الجريمة، في حين أن القصد الخاص لا يكتفي بذلك، وإنما يتطلب عنصرًا يضاف إليهما، ويفترض لتوافر القصد الخاص ثبوت توافر القصد العام، وتتطلب بعض النصوص التي جرمت الدخول غير المصرح به إلى نظام الحاسب الآلي في التشريعات المختلفة قصدًا خاصًا إلى جانب القصد العام، وقد يترتب على توافر هذا القصد تشديد العقوبة، ففي الدنمارك على سبيل المثال تشدد العقوبة متى ارتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات، وفي أستراليا يوجد نص خاص يشدد العقوبة متى ارتكب فعل الدخول غير المصرح به إلى نظام الحاسب

(1) د. فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية، مرجع سابق، ص235.

الآلي بنية الإضرار بالغير، وفي النرويج تشدد العقوبة على نحو ملحوظ متى ارتكب فعل الدخول غير المصرح به بنية حصول الفاعل - له أو للغير - على ربح غير مشروع أو إلحاق ضرر بالغير نتيجة للاطلاع على المعلومات التي يحتوي عليها النظام.

أما القانون البرتغالي فيتطلب قصدًا خاصًا للعقاب على الدخول غير المصرح به، فالمادة السابعة من القانون البرتغالي بشأن جرائم المعلوماتية لعام 1991، تعاقب كل من يقوم على نحو غير مصرح به بالدخول إلى نظم شبكات المعلومات بنية الحصول له أو للغير على ربح أو فائدة غير مشروعة، وتشدد العقوبة متى كان هذا الربح أو هذه الفائدة مرتفعين بصورة كبيرة نسبيًا، وقد انتقد الفقهاء النص البرتغالي لتضييقه على نحو كبير لتطبيق جريمة الدخول غير المصرح به، ويرى البعض أنه لتفادي هذا التضييق يجب أن تفسر الفائدة التي يحصل عليها الفاعل لتشمل إلى جانب الفائدة المادية، كل فائدة ذهنية أو معنوية قد يحصل عليها الفاعل من وراء دخوله إلى النظام، وألا تقتصر الفائدة على الربح المادي.

ويتضمن قانون إساءة استخدام الحاسبات الآلية في المملكة المتحدة لعام 1990 في مادته الثانية[1] نصًا يجرم الدخول غير المصرح به متى توافر لدى الفاعل قصد خاص يتمثل في نية ارتكاب جريمة أخرى لاحقة على هذا الدخول، فإلى جانب المادة الأولى من هذا القانون والتي تجرم الدخول غير المصرح به إلى نظام الحاسب الآلي، جاءت المادة الثانية بجريمة أخرى عرفت باسم الدخول غير المصرح به إلى نظام الحاسب الآلي بنية ارتكاب أو تسهيل ارتكاب جرائم أخرى، وقد جاءت هذه المادة لتعالج الحالات التي يرتكب فيها الدخول غير المصرح به إلى نظام الحاسب الآلي بنية ارتكاب

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 179.

جريمة أخرى كالسرقة أو التهديد أو النصب، إلا أن هذه الجريمة لا يمكن العقاب عليها بوصف الشروع نظرًا لعدم إتيان الفاعل عملا يعد بدءًا في تنفيذها، ويتعين لقيام هذه الجريمة أن تتوافر لديه نية ارتكاب جريمة أخرى.[1]

---

(1) Section 1.(1) A person is guilty of an offence if،
(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
(b) the access he intends to secure is unauthorized; and
(c) he knows at the time when he causes the computer to perform the function that that is the case.
(2) The intent a person has to have to commit an offence under this section need not be directed at،
(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.
(3) A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.
Section 2 2.(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorized access offence")with intent
(a) to commit an offence to which this section applies; or
(b) to facilitate the commission of such an offence (whether by himself or by any other person);and the offence he intends to commit or facilitate is referred to below in this section as the further offence.
(2) This section applies to offences،
(a) for which the sentence is fixed by law; or
(b) for which a person of twenty،one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).
(3) It is immaterial for the purposes of this section whether =

وقد أوضحت هذه المادة في فقرتها الثالثة أنه لا يشترط أن تتزامن نية الدخول إلى نظام الحاسب الآلي مع نية ارتكاب جريمة أخرى، كما ذكرت المادة الثانية في فقرتها الرابعة أنه لا يغير في الأمر أن يكون ارتكاب الجريمة الثانية مستحيلا، ويعاقب الفاعل وفقًا للفقرة الخامسة من المادة الثانية بالحبس الذي لا يتجاوز خمس سنوات.[1]

وفي قانون مكافحة جرائم تقنية المعلومات الإماراتي شاهدنا المادة (22) والتي اشترطت قصدًا خاصًا عندما جرمت كل من دخل وبغير وجه حق موقعًا أو نظامًا، مباشرة أو عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، بقصد الحصول على بيانات أو معلومات حكومية سرية، إما بطبيعتها أو بمقتضى تعليمات صادرة بذلك، إذا ترتب على الدخول إلغاء تلك البيانات أو المعلومات أو إتلافها أو تدميرها أو نشرها، وتكون العقوبة السجن مدة لا تقل عن خمس سنوات، ويسري حكم هذه المادة على البيانات والمعلومات الخاصة بالمنشآت المالية والمنشآت المالية الأخرى والتجارية والاقتصادية.

كما نصت المادة (14) على عقوبة كل من دخل بدون وجه حق موقعًا

= the further offence is to be committed on the same occasion as the unauthorized access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

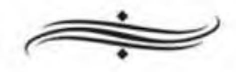
1) Section 2 (5) A person guilty of an offence under this section shall be liable،

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

في الشبكة المعلوماتية لتغيير تصاميم هذا الموقع أو إلغائه أو إتلافه أو تعديله أو شغل عنوانه.

وأخيرا يمثل الركن المعنوي بالمفهوم العام اتجاه إرادة الجاني إلى إقامة الاتصال غير المشروع بالنظام الآلي لمعالجة البيانات، في حين أن القصد الخاص يمتاز بأن العلم والإرادة لا يقتصران على أركان الجريمة وعناصرها، وهي هنا الدخول والبقاء في النظام، وإنما يمتدان بالإضافة إلى ذلك إلى وقائع ليست في ذاتها من أركان الجريمة، وتوافر هذا القصد الجنائي بهذه الصورة من عدمه هو مسألة موضوعية يقدرها قاضي الموضوع على ضوء الوقائع الثابتة أمامه من خلال أوراق الدعوى، ونشير أخيرًا إلى ضرورة أن يكون القصد الجنائي معاصرًا للنشاط الإجرامي، بمعنى أن تكون إرادة الجاني المتجهة إلى فعل الدخول غير المشروع على مواقع التجارة الإلكترونية معاصرة للفعل ذاته، فإذا تخلفت هذه الإرادة عن الفعل المادي انتفت عن ذلك الفعل الصفة الإجرامية وفقًا للقاعدة العامة في القانون الجنائي.[1]



(1) د. فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية، مرجع سابق، ص235.

المبحث الثاني

جريمة إتلاف وتدمير مواقع التجارة الإلكترونية

تعد جريمة إتلاف المعلومات من الجرائم المنتشرة في فضاء شبكة الإنترنت، وهذه الجريمة قد تأخذ عدة صور، إما أن يكون الفعل المجرّم فيها هو إتلاف البيانات والمعلومات، ويتم ذلك الفعل المؤثم بتشويه البرامج أو المعلومات على نحو يجعلها غير صالحة للاستعمال[1]، وتتمثل الصورة الثانية في حالة تمكن الجاني من الدخول إلى حاسب آلي خاص لشخص آخر وتغيير البيانات أو المعلومات أو البرامج بالزيادة أو النقصان أو الحذف أو الإضافة، وفي هذه الحالة تعتبر الجريمة متوافرة، ويعاقب عليها الجاني حتى لو لم يترتب على تغير البيانات أو المعلومات ضرر، وذلك لأن الحماية مقررة لصالح المجني عليه وجهازه، وقد يتمثل أخيرًا الفعل الإجرامي في محو البيانات أو المعلومات أو البرامج، بحيث يجعلها كأن لم تكن بما يؤدي إلى حرمان صاحب الجهاز من استعمال البيانات أو المعلومات أو البرامج[2].

وقد جاء تجريم هذه الأفعال في نص الفقرة الثانية من المادة الثانية من قانون مكافحة جرائم تقنية المعلومات الإماراتي، على أنه إذا ترتب على الفعل إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات فيعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة، أو

(1) د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص 43, وانظر في ذات الموضوع لذات المؤلف: الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص11.

(2) د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2002، ص 43.

بإحدى هاتين العقوبتين.

ويعاقب هذا النص على صور جريمة الإتلاف المعلوماتي لنظام المعالجة الآلية للبيانات، سواء تضمن ذلك إتلافها أو الإلغاء أو الحذف، أو التدمير، وهي صور متعددة تؤدي إلى الإتلاف، أو تغيرها أو محوها، سواء كانت بيانات أو معلومات مخزنة بالحاسب الآلي، أو برامج.

والإتلاف هو تعييب الشيء على نحو يفقده قيمته الكلية أو الجزئية، وذلك إذا كان الفعل قد أفقد قيمة الشيء كلها أو جزءًا منها، فقد تحقق الاعتداء الذي يجرمه القانون، فهو إفناء لمادة الشيء أو على الأقل إحداث تغيير شامل عليها، بحيث يصير غير صالح إطلاقًا للاستعمال في الغرض المخصص له، ومن ثم تضيع قيمته على المالك[1].

وقد عاقبت القوانين التقليدية القائمة كالقانون الفرنسي على الإتلاف العمدي بنص المادة (323) عقوبات، والمادة (424) من قانون العقوبات الإماراتي، والمشرع المصري المادة (361) عقوبات، كما عاقبت القوانين المتخصصة في الجرائم المعلوماتية على الإتلاف المعلوماتي كقانون مكافحة جرائم تقنية المعلومات الإماراتي، وسنتناول في هذا المبحث صور الإتلاف والتدمير، والإتلاف المعنوي، وأركان الجريمة، والفيروسات، وموقف التشريعات، وسنحاول أن نرى مدى استطاعة النصوص التقليدية القائمة مواجهة الجريمة المعلوماتية في هذا المجال، وذلك في المطلبين الآتيين:

المطلب الأول: أركان جريمة الإتلاف

المطلب الثاني: الإتلاف المعلوماتي وحماية التجارة الإلكترونية

(1) د. محمود نجيب حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، دراسة مقارنة،1984، ص 196.

المطلب الأول

أركان جريمة الإتلاف

جريمة الإتلاف قد تقع عن طريق شبكة الإنترنت، وذلك بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وعن طريق التعدي على البرامج والبيانات المخزنة والمتبادلة عن طريق شبكة الإنترنت، والتلاعب بالبيانات وإتلاف المعلومات المخزنة بالحواسيب بمحوها أو تعديلها أو تغيير نتائجها، أو التشويش على النظام المعلوماتي، وإعاقة سير عمل النظام.

وبالتالي يكون الإتلاف العمدي للبرامج والبيانات بمحوها كلية، أو تدميرها إلكترونيًا، أو تشويشها على نحو فيه إتلاف بما يجعلها غير صالحة للاستعمال[1].

وتستلزم نصوص قانون العقوبات في فرنسا والإمارات العربية المتحدة ومصر لقيام جريمة الإتلاف لزوم توافر أركانها من فعل مادي هو الإتلاف، ووقوع فعل الإتلاف على محل مادي أو معنوي (وفقا لما سنرى) مملوك لغير الجاني، وتوافر القصد الجنائي باعتبارها جريمة من الجرائم العمدية، وسوف نعرض فيما يلي لكل ركن من هذه الأركان:

(1) د. هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان [الجرائم الواقعة في مجال تكنولوجيا المعلومات] القاهرة، 25- 28 أكتوبر 1993، دار النهضة المصرية، ص 558.

الفرع الأول

الركن المادي للإتلاف

يتمثل في تخريب الأموال بجعلها غير صالحة للاستخدام والاستعمال، ولا يشترط القانون أن يكون الإتلاف تامًّا بل تقوم الجريمة ولو كان جزئيًّا، ويشترط القانون في حالة الإتلاف الجزئي أن يكون فعل الإتلاف من شأنه جعل المال غير صالح للاستعمال، أو تعطيله بأية طريقة[1]، وهو أمر يقدره قاضي الموضوع وفقًا لظروف كل حالة على حدة[2]، ويحدد قانون العقوبات المصري[3] محل جريمة الإتلاف بأنه التخريب والإتلاف العمدي

---

(1) تنص المادة (424) إماراتي على أنه: (يعاقب بالحبس مدة لا تزيد على سنة، وبالغرامة التي لا تجاوز عشرة آلاف درهم، أو بإحدى هاتين العقوبتين كل من هدم أو أتلف مالا مملوكا للغير ثابتا كان أو منقولا جعله غير صالح للاستعمال أو عطله بأية طريقة، وتكون العقوبة الحبس إذا نشأ عن الجريمة تعطيل مرفق عام أو منشأة ذات نفع عام، أو إذا ترتب عليها جعل حياة الناس أو أمنهم أو صحتهم في خطر، وتكون العقوبة السجن مدة لا تزيد على خمس سنوات إذا وقعت الجريمة من عصابة مؤلفة من ثلاثة أشخاص على الأقل).

(2) د. رمسيس بهنام، شرح قانون العقوبات، القسم الخاص، 1982، ص 443.

(3) تنص المادة (361) من قانون العقوبات المصري على أن: "كل من خرب أو أتلف أموالا ثابتة أو منقولة لا يمتلكها، أو جعلها غير صالحة للاستعمال، أو عطلها بأية طريقة يعاقب بالحبس مدة لا تزيد على ستة أشهر وبغرامة لا تجاوز ثلاثمائة جنيه أو بإحدى هاتين العقوبتين، فإذا ترتب على الفعل ضرر مالي قيمته خمسون جنيهًا أو أكثر كانت العقوبة الحبس مدة لا تجاوز سنتين وغرامة لا تجاوز خمسمائة جنيه أو إحدى هاتين العقوبتين، وتكون العقوبة السجن مدة لا تزيد على خمس سنين وغرامة لا تقل عن مائة جنيه ولا تجاوز ألف جنيه إذا نشأ عن الفعل تعطيل أو توقيف أعمال مصلحة ذات منفعة عامة، أو ترتب عليه جعل حياة الناس أو صحتهم أو أمنهم في خطر، ويضاعف الحد الأقصى للعقوبات إذا ارتكبت الجريمة =

للأموال سواء منها ما كان ثابتًا أو منقولا، بشرط أن تكون مملوكة للغير، ويستلزم القانون لوقوع هذه الجريمة إلى جانب ذلك ضرورة توافر القصد الجنائي.

وتتحقق هذه الحماية عن طريق حماية موضوع المال نفسه حفاظًا على منفعته، بمعنى أن فعل التجريم يهدف إلى الحفاظ على القيمة الاقتصادية للشيء، وعلى ذلك فإن الاعتداء على المال يعد بمثابة إتلاف إذا أفقده خاصية استعماله رغم بقاء مادة الشيء[1]، لأن العبرة في إتلاف الشيء هو إنقاص قيمته؛ لأن محل الحماية الحقيقي هو قيمة الشيء، وليست حماية مادته إلا وسيلة لحماية قيمته، وإذا كان الفعل المجرم قد أفقد الشيء قيمته إذا انتقص منه فقد تحقق الاعتداء الذي يعاقب عليه القانون باعتباره قد ذهب بأهمية الشيء بالنسبة لمالكه.

ويقع الإتلاف على الأموال المادية سواء أكانت عقارات أو منقولات، ويستوي في المنقولات أن تكون أموالا مادية أو أموالا معنوية، كخطابات ذات قيمة بالنسبة لصاحبها، أو برامج معلوماتية، أو كيانات خاصة بالحاسب الآلي.

وقد نصت المادة (424) عقوبات إماراتي والسابق ذكرها على أربع صور للفعل الذي يقوم به الركن المادي لجريمة الإتلاف، وهذه الصور هي هدم المال، إتلاف المال، جعل المال غير صالح للاستعمال، وتعطيل المال بأية طريقة.

والصور الأربع تكاد تكون مرتبطة مع بعضها البعض، فقد يقع الإتلاف

= تنفيذًا لغرض إرهابي".

(1) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 1992، ص127.

على جزء من المال وتقوم الجريمة بشرط أن يكون من شأن هذا الإتلاف جعل المال غير صالح للاستعمال أو تعطيله.

كما أن المشرع هنا لم ينص على وسيلة محددة لفعل الإتلاف، وبالتالي تقع الجريمة بأي فعل من شأنه تعطيل المال محل الجريمة أو تعييبه وجعله غير صالح للاستعمال بعد ذلك.

ويشترط في محل الجريمة أن يكون مالا سواء أكان منقولا أو عقارًا إلا ما خرج من حكمه بنص آخر، فقد نص قانون العقوبات على أحوال كثيرة أخرجها من حكم المادة (424) وفرض لها عقوبات خاصة، ومن أمثلتها إتلاف الأوراق أو الوثائق المتعلقة بأمن الدولة أو بأية مصلحة وطنية أخرى (المادة 155 / 2)، وإتلاف سلاح أو سفينة أو طائرة أو مهمات أو منشأة أو وسيلة مواصلات أو مرفق عام أو ذخيرة أو مؤن أو أدوية، أو غير ذلك مما أعد للدفاع عن الدولة ويستعمل في ذلك (المادة 161)، وإتلاف مستند من شأنه تسهيل كشف جريمة من الجرائم المنصوص عليها في الفصل الأول من الكتاب الثاني الخاص بالجرائم الماسة بالأمن الخارجي للدولة (المادة 3/171)، وإتلاف مبان أو أملاك عامة أو مخصصة لدوائر حكومية أو غيرها من الجهات (المادة 1/190)، وإتلاف أو هدم المنشآت أو الوحدات الصحية المتنقلة أو المواد أو الأدوات الموجودة فيها، أو تعطيل شيء فيها، أو جعله غير صالح للاستعمال (المادة 4/190)، وإتلاف الأختام الموضوعة بناءً على أمر من السلطة القضائية أو الجهات الإدارية (المادة 1/277)، وإتلاف أوراق ومستندات أو أشياء محجوز عليها قضائيًا أو إداريًا (المادة 278)، وتخريب أو إتلاف طريق أو مطار أو قنطرة أو مجرى مياه صالح للملاحة (المادة 290)، وإتلاف شيء من أسلاك وسائل الاتصال السلكية واللاسلكية المخصصة لمنفعة عامة أو أجهزتها (المادة

297)، وإتلاف الآلات أو الأنابيب أو الأجهزة الخاصة بمرفق المياه أو الكهرباء أو الغاز أو البترول (المادة 301)، وإتلاف المنشآت الصحية الثابتة أو الوحدات الصحية المتنقلة أو المواد أو الأدوات الموجودة فيها (المادة 302).

والمال الذي وقع عليه فعل الإتلاف يجب أن يكون مملوكًا لغير الجاني حتى تقوم جريمة الإتلاف قانونًا، فإذا كان المال مملوكًا للجاني فلا جريمة على اعتبار أن له حق التصرف المطلق في ماله، بشرط أن تكون ملكيته للشيء المتلف خالصة.

كما جاء النص على هذه الجريمة في المادة (361) من قانون العقوبات المصري، والمادة (323) من قانون العقوبات الفرنسي[1].

وباستقراء هذه النصوص نجد أنها تعاقب على جرائم الإتلاف العمدي للعقار أو المنقول ذي الطبيعة المادية، كما أنها من الممكن أن تمتد إلى تجريم إتلاف الكيانات المنطقية والبرامج والمعلومات، أو ما يعرف بالجريمة المعلوماتية[2] في حالة غياب التشريعات الخاصة، حيث إن هذا النوع من الجرائم ليس حديثًا، فالجريمة المعلوماتية لها جذور في قانون العقوبات المقارن، من حيث إنه يحتوي على مجموعة من الجرائم محلها

---

(1) النص الفرنسي لا يخرج عن مفهوم نص المادتين السابق بيانهما، راجع في القانون الفرنسي:

- Ander Iucas، le driot de l'informatique henis droit، press universitaitrem frqance، Paris، 1987، P: 521 et ss.

- مشار إليه لدى د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص 43 وما بعدها.

(2) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 257.

المعلومات، كما هو الحال في جرائم التجسس والتخابر، والحصول على وثائق وأسرار الدفاع، والحصول على الاكتشافات العلمية والابتكارات الصناعية[1]، وقد تضمنت المادة 323 من قانون العقوبات الفرنسي[2] عقاب كل من قام بإتلاف المال المعلوماتي المادي، مثل آلات وأدوات الحاسب الآلي[3]، ويجب التفرقة بين نوعين من هذا المال في نطاق تجريم إتلاف المال المعلوماتي:

- الأموال المادية مثل جهاز الحاسب الآلي وملحقاته.
- الكيانات المنطقية والبرامج وغيرها من البيانات وهي أموال "لا مادية"[4].

وبناءً على ذلك فإن النصوص تعاقب على إتلاف النوع الأول من الأموال المعلوماتية وهي الأموال المادية، مثال ذلك إتلاف أجهزة الحاسب الآلي وملحقاتها من الطابعة والماسح الضوئي، وكذلك جميع الأجهزة الملحقة بالكمبيوتر، وشاشة الكمبيوتر والكاميرا الملحقة به، وأي وصلات أو

(1) د. عمر أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 221.

(2) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول،الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، ص 130.

(3) د. هدى حامد قشقوش، الإتلاف العمدي لبرامج الحاسب الآلي، دار النهضة العربية، القاهرة، 1997، ص7.

(4) يلاحظ أن الاعتراف لهذه الكيانات بصفة المال أثارت جدلا في الفقه والقضاء، د. عبد الفتاح مراد، التجارة الإلكترونية والبيع والشراء على شبكة الإنترنت، الهيئة القومية لدار الكتب والوثائق المعدلة، القاهرة، 2004، ص280, وفي المعنى ذاته: د. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من1، 3 مايو2000، ص 11.

معدات مجهزة للاستخدام عن طريق الحاسب الآلي، أي كل ما ينطبق عليه وصف الشيء المادي المنقول، فكل هذه الأشياء تخضع للحماية المقررة في المادة (361) من قانون العقوبات المصري، وكذلك المادة (323) من قانون العقوبات الفرنسي، والمادة رقم (424) من قانون العقوبات الإماراتي.

والمشرع الإماراتي وكذا المصري قد تناولا الإتلاف إذا ما وقع على مال ثابت أو منقول مملوك للغير، فإذا كان محل الإتلاف جهاز الحاسب الآلي أو أدواته أو الأجهزة المتصلة به أو الأشرطة أو الأقراص الممغنطة أو الدعامات، أو غيرها مما يختص بالمعلومات وله كيان مادي فإنه لا تثار أي عقبة قانونية في تطبيق النصوص التقليدية الخاصة بجريمة الإتلاف، على اعتبار أن محل الجريمة مال مادي مملوك للغير.

ولكن قد تثور مشكلة المعلومات الموجودة بداخل أجهزة الحاسب الآلي والتي تم إتلافها بإتلاف الحاسب الآلي أو ملحقاته، أو إتلاف المعلومات وحدها دون المساس بالأشياء المادية، فهل تسري النصوص التقليدية الخاصة بالإتلاف على المعلومات والبيانات الموجودة بالجهاز إذا ما تلفت بإتلاف الجهاز الذي يحتويها، أو إذا تم إتلافها بصورة مباشرة عن طريق برامج الفيروسات وغيرها.

انقسم الفقه إزاء ذلك إلى رأيين، الأول يرى أن جريمة الإتلاف لا تقع إلا على الأموال المادية دون المعنوية، فلا يدخل إتلاف المعلومات ضمن التجريم المنصوص عليه في النصوص التقليدية الخاصة بالإتلاف[1].

أما الرأي الثاني فقد ذهب إلى الأخذ بعموم اللفظ؛ حيث إن المشرع نص على حماية الأموال ثابتة أو منقولة، والمال المنقول نوعان مادي ومعنوي،

(1) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 156.

وبالتالي تشمله الحماية الجنائية المقررة وفقًا للنصوص القائمة.

وكذلك المعلومات الموجودة على الأجهـزة الماديـة تكـاد أن تكـون جـزءًا لا يتجـزأ مـن هـذا الجهاز، ومن المحتمل أن تكون قيمة الجهاز مستمدة من وجود المعلومات عليه.

كما يلاحظ أن القانون لم يجرم نتيجة واحدة محددة، وإنما جـرّم التخريـب والإتـلاف وعـدم الصلاحية للاستعمال والتعطيـل، ويقصـد بـالإتلاف إفنـاء مـادة الشيـء أو هلاكـه كليًـا أو جزئيًـا، ويقصد بالتخريب توقف الشيء تمامًا عن أن يؤدي منفعته حتى ولـو لم تفـن مادتـه سـواء أكـان هذا التوقف كليًا أم جزئيًا، ويقصد بعدم الصلاحية للاسـتعمال جعـل الشيـء لا يقـوم بوظيفتـه المنوطة به على النحو الأكمل، أما التعطيل فيقصد بـه توقـف الشيـء عـن القيـام بوظيفتـه فـترة مؤقتة، ويكفي تحقق إحدى هذه النتائج الأربعة بالفعل للقول بتوافر الجريمة[1].

يتضح لنا مما سبق أن المشرع قصد من وراء تجريم الإتلاف بتحقيق إحدى النتائج السـابقة ليس فقط حماية مادة الشيء وإنما بالدرجة الأولى حماية قيمته الاقتصادية والتجارية، حيث مـن المتصور وقوع الجريمة رغم بقاء مادة الشيـء إذا نجـم عـن السـلوك الإجرامـي انتقـاص أو فنـاء القيمة الاقتصادية، بأن جعله غير صالح للاستعمال، أو قلل من قوته في المبادلة التجارية.[2]

(1) د. علي عبد القادر القهوجي، الحماية الجنائيـة للبيانـات المعالجـة إلكترونيـا، بحـث مقـدم لمؤتمر القـانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، 1 - 3 مايو 2000، ص 35.

(2) د. محمود نجيب حسني، جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، مرجع سابق، ص 487.

ويميل الباحث إلى ما ذهب إليه أصحاب الرأي الثاني من خضوع المعلومات والبيانات الموجودة داخل أجهزة الحاسوب إذا ما أتلفت هذه الأجهزة للحماية الجنائية طبقًا للنصوص التقليدية التي تجرم الإتلاف، خصوصًا وأن المشرع لم يحدد طريقة بعينها لوقوع الجريمة، ولم يحدد نتيجة واحدة محددة لقيامها، لأن من شأن ذلك حماية البيانات، وخوفا من إفلات المجرمين من العقاب.

وبالتالي فإنه تخضع لهذه الحماية البرامج والمعطيات الخاصة بالحاسب الآلي متى كانت مسجلة على دعامة، ففي هذه الحالة فقط يمكن القول بأنها منقول مادي ذو قيمة لدى مالكها أو صاحبها، أما لو كانت ذات طبيعة غير مادية، فهي ستدخل ضمن المال المعلوماتي، أي ضمن الكيانات المنطقية التي لا زالت تثير خلافًا في الفقه حول طبيعتها ومدى كونها من الأموال المنقولة أم لا.[1]

وتتعدد أشكال وحالات وصور الاعتداء المادي المعلوماتي وتتنوع، ونورد بعض هذه الحوادث والأمثلة وفقا لما يلي:[2]

- في أول السبعينيات في الولايات المتحدة الأمريكية تم تدمير العديد من الحاسبات الآلية بواسطة جماعات مناهضة لحرب فيتنام، بل حدث وأن توفي شخص واحد، وأصيب ثلاثة بإصابات خطيرة عندما ألقيت قنبلة على الحاسب الآلي التابع لمركز أبحاث القوات المسلحة بجامعة Wisconsin وعلى ذلك تكون الحاسبات الآلية ضحية للدعاية

(1) د. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق، ص 20.
(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 97 وما بعدها.

المناهضة للولايات المتحدة الأمريكية.

- وفي إيطاليا وخلال عامي 1976، 1977 قامت مجموعة إرهابية إيطالية بتدمير اثني عشر حاسبًا تابعًا لمصلحة الضرائب، وذلك باستخدام الفتيل وخليط المولوتوف، كما قامت منظمة الألوية الحمراء في إيطاليا بارتكاب العديد من أفعال التعدي ضد مراكز المعلوماتية، وتسببت في خسائر قدرت بمليون دولار في كل حادث.
- في عام 1980 قامت جماعة إرهابية تعرف باسم منظمة العقل المباشر بتدمير البرامج والبطاقات الخاصة بمنشأة صناعية كبرى متخصصة في بيع الحاسبات الآلية وترتيب المعلومات المحاسبية لعدد من الشركات.
- في ألمانيا عام 1983 قامت مجموعة بالهجوم بالقنابل على مركز Man للحاسبات الآلية، وذلك احتجاجًا على اشتراك هذه الشركة في إنتاج صواريخ Pershing مما ترتب على ذلك خسائر قدرت بحوالي مليون مارك.[1]
- في فرنسا أعلنت لجنة Clodo مسئوليتها عن أفعال التعدي ضد الشركات الرئيسية للمعدات المادية المعلوماتية خاصة في إقليم تولوز الفرنسي، وترتب على ذلك خسائر قدرت بحوالي عشرات الملايين من الفرنكات الفرنسية.[2]

ويرى الفقه الجنائي أن مصادر الاعتداء على المعدات المعلوماتية

(1) د. هشام فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 152.
(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 100.

المادية وإتلافها عديدة ومتنوعة[1]، وكذلك بواعث هذا الاعتداء تبدو كذلك متنوعة، وتختلف من شخص إلى آخر.[2]

ونخلص من ذلك إلى تصور تجريم الإتلاف المادي للمنقولات المعلوماتية كأجهزة الحاسب الآلي وملحقاته، وذلك استنادًا للنصوص التقليدية كالمادة (361) من قانون العقوبات المصري، وكذلك المادة (323) من قانون العقوبات الفرنسي والمعدلة بالقانون الصادر عام 1988، والمادة (424) من قانون العقوبات الإماراتي.

أما عن النوع الثاني من الأموال المعلوماتية، وهي الأموال غير المادية كالبرامج والكيانات المنطقية والبيانات والمعلومات المعالجة، فإن أغلبية الفقه الجنائي يرى خضوع هذه الأموال لفعل الإتلاف رغم أنها ليست من الأشياء المادية، فالمعلومات ذات قيمة اقتصادية، ويمكن نقلها ويمكن تدميرها وإتلافها عن طريق التدخل في هذه البرامج وهي محملة على جهاز الحاسب الآلي، ويمكن إتلافها كليًا أو جزئيًا أو تشويهها، ومن ثم فإن هذه المعلومات تخضع لنصوص تجريم الإتلاف.[3]

---

(1) تتعدد مصادر هذا الاعتداء المسبب للإتلاف، فقد تكون الطبيعة كما في ارتفاع الحرارة المفاجئ، والفيضانات والزلازل، التي تتسبب في الإتلاف، وقد يكون مصدر الإتلاف هو الإنسان نفسه.

(2) تتعدد بواعث الإتلاف وتتنوع كعدم رضاء المستخدمين عن أصحاب أعمالهم، مثلما حدث في النرويج حيث أتلفت حاسبات آلية لشركة عقب فصل عشرين مستخدمًا كانوا يعملون بها. كما قد يتم تدمير الحاسبات الآلية بطريق الخطأ، انظر د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 97.

(3) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 35. وفي المعنى ذاته: د. غنام محمد غنام، عدم ملاءمة القواعد =

هذا وقد ذهب القضاء الفرنسي في تطبيق جريمة إتلاف المكونات المنطقية لأنظمة الحاسب الآلي إلى اعتبار هذه الصورة مكونًا لهذه الجريمة، حيث أدانت محكمة استئناف باريس عام 1990 أحد الأشخاص بتهمة إتلاف المعلومات لقيامه بإدخال بيانات غير صحيحة إلى نظام الحاسب الآلي، كما ذهبت محكمة جنح ليموج عام 1994م إلى إدانة المتهم بتهمة إتلاف المكونات المنطقية للحاسب الآلي لقيامه بإدخال برنامج خبيث "حصان طروادة" إلى نظام الحاسب الآلي مما ترتب عليه إتلاف للمعلومات، فضلا عن إعاقة النظام عن أداء وظائفه، كما ذهبت محكمة النقض الفرنسية في حكم لها عام 1996م إلى أن إدخال البرامج الخبيثة إلى نظام الحاسب الآلي هو سلوك معاقب عليه طبقًا للفقرة الثانية من المادة 323 من قانون العقوبات، كما ذهبت نفس المحكمة أيضًا في حكم لها صادر عام 1999 إلى أن إدخال بيانات يترتب عليها إتلاف لأي من المكونات المنطقية لنظام الحاسب الآلي هو سلوك معاقب عليه ولو كان للجاني حق الدخول إلى هذا النظام[1].

وعلى صعيد النصوص الخاصة شاهدنا الفقرة الثانية من المادة الثالثة من قانون مكافحة جرائم تقنية المعلومات الإماراتي عاقبت على جريمة الإتلاف المعلوماتي، فنصت على صور هذا الإتلاف، وهو الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أو التغيير أو إعادة نشر بيانات أو معلومات.

والأموال محل الحماية هنا قد تصدق على البرامج والبيانات والمعلومات، وقد تشمل أيضًا نظام المعالجة الآلية للبيانات بمكوناته المادية

= التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق، ص 20.

(1) د. نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية، مرجع سابق، ص 223.

من جهاز الحاسب الآلي وملحقاته وغيرها.[1]

ويعد من قبيل الظروف المشددة في العقاب على هذه الجريمة، إذا وقعت الجريمة على بيانات شخصية.

ويلحق بالركن المادي أيضًا بالإضافة لما سبق الإتلاف عن طريق الإدخال العمدي للبيانات، وكذلك تعديل عملية طرق معالجة البيانات أو طريقة نقلها، وهو ما يعني تغيير النظم المعلوماتية والبرامج التي يعمل بها هذا النظام.

ونخلص من ذلك إلى أن المشرع الإماراتي قد قنن ما استقر عليه الفقه وكذلك القضاء في شأن تجريم الإتلاف المعلوماتي.

ويرى الفقه الجنائي أن المشرع لم يحدد طريقة بعينها لوقوع جريمة الإتلاف أو إحدى صوره، وإن اعتبره جريمة لاحقة على الدخول غير المشروع، ولم يحدد نتيجة واحدة محددة لقيامها، ولذلك فمن المتصور أن يتجه الجاني بنشاطه الإجرامي إلى البرنامج والدعامة المسجل عليها معًا، أو إلى البرنامج فقط دون الدعامة، وقد تقع الجريمة عن طريق الاتصال المباشر بالجهاز، كما قد تقع من خلال الاتصال عن بعد.[2]

(1) ويقصد بنظام المعالجة الآلية للبيانات: "كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة، سواء أكانت متمثلة في ذاكرة الحاسب وبرامجه، أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة".

(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 26، ويذكر أن الفقه الفرنسي يستخدم مصطلح degradation للتعبير عن الإتلاف المادي الذي يلحق بالمعدات المادية لنظم المعلومات، ومصطلح alteration للإشارة إلى الإتلاف المعنوي الذي يصيب محتويات الكيانات المنطقية والبيانات المعالجة.

ويرى جانب من الفقه أن المادة (323) من قانون العقوبات الفرنسي[1] تجرم الإتلاف المادي المعلوماتي لأجهزة الحاسب الآلي وملحقاته أيضًا[2]، حيث جاء نص المادة (1/323) معاقبًا على (الدخول أو البقاء، بطريق الغش، داخل كل أو جزء من نظام المعالجة الآلية للمعطيات يعاقب عليه بالحبس لمدة سنة وغرامة مقدارها (100.000) فرنك، فإذا نجم عن هذا الدخول محو أو تعديل في المعطيات المختزنة في النظام أو إتلاف تشغيل هذا النظام تكون العقوبة الحبس لمدة سنتين وغرامة مقدارها (200.000) فرنك).

ونص في المادة (2/323) على أن (تعطيل أو إفساد نظام تشغيل نظام المعالجة الآلية للبيانات يعاقب عليه بالحبس لمدة ثلاث سنوات وغرامة مقدارها 300.000 فرنك).

كما نص في المادة (3/323) على أن (إدخال البيانات بطريق الغش في نظام المعالجة الآلية، أو محوها، أو التعديل بطريق الغش للمعطيات التي يحتويها، يعاقب عليه بالحبس لمدة ثلاث سنوات وبغرامة مقدارها 300.000 فرنك).

فالمشرع الفرنسي عاقب على الدخول بطريق التدليس إلى نظام المعالجة الآلية للمعلومات، كما شدد على الجاني إذا ما نشأ عن هذا الدخول محو أو تعديل في المعطيات المخزنة في النظام، أو إتلاف تشغيل النظام وفقًا للفقرة الأولى من المادة السابقة.

---

(1) يقابلها نص المادة (2/462) من نصوص القانون رقم 19 لعام 1988.

(2) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص 78, وفي المعنى ذاته د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 130.

كما عاقب على تعطيل أو إفساد نظام التشغيل كما ورد في الفقرة الثانية، وتطبيقًا لهذا النص قضي بإدانة متهم قام بإدخال فيروس في أحد أنظمة المعالجة الآلية للمعلومات عن طريق وضع فيروس على أسطوانات إعلانية تحتوي على ملخص لبرنامج يراد الترويج له، ثم وزع هذه الأسطوانات مع أعداد جريدة متخصصة في مجال المعلوماتية، وباستخدام هذه الأسطوانات تم نقل الفيروس إلى نظام التشغيل فأتلف المعلومات[1].

وقد جاءت الفقرة الثالثة من المادة (323) من قانون العقوبات الفرنسي الجديد لتعاقب بصريح النص على إتلاف المعلومات الموجودة في الذاكرة أو على الأسطوانة، وذلك كأن يقوم الجاني بإدخال بيانات تؤدي إلى شغل الذاكرة بالكامل، وتعجز بالتالي عن التعامل مع المعطيات، أو تؤدي إلى إتلاف المعلومات الموجودة بداخل النظام، وحدد ثلاث صور لذلك وهي الإدخال والمحو والتعديل، ويقصد بالإدخال إضافة معطيات جديدة على الدعامة الخاصة سواء كانت خالية أم كان يوجد عليها معطيات، أما المحو فهو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام، أو تحطيم تلك الدعامة، أو نقل وتخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة، أما التعديل فيتحقق بتغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى.[2]

أما التشريع الأمريكي والصادر عام 1984 فلم يحتو على ما من شأنه تجريم إتلاف البيانات والمعلومات والبرامج بصورة عامة, وإنما اقتصر التجريم فقط على الإتلاف الذي يترتب عليه إعاقة أنظمة الحاسبات الآلية

(1) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 62.
(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيًا، مرجع سابق، ص 37.

عن العمل, حيث جاءت الفقرة الثانية من المادة 1030- أ لتنص على تجريم إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية.

إلا أنه نتيجة لكثرة الانتقادات التي وجهت إلى هذا التشريع فقد تم تعديله بحيث أصبحت الفقرة الثالثة من المادة 1030- أ تتناول فقط الدخول غير المصرح به إلى حاسب آلي تستعمله الحكومة متى أعاق الدخول هذا الاستعمال، وأضيفت فقرة خامسة إلى ذات المادة جرّمت الإتلاف العمدي غير المصرح به لمعلومات يحتويها حاسب آلي تابع لحكومة الولايات المتحدة وإدارتها، أو حاسب آلي غير تابع للحكومة إلا أنه يتم استخدامه من قبلها أو لصالحها، أو إعاقة هذا الحاسب عن إدارة المهام المختلفة التي تباشرها الحكومة بواسطته.

والهدف من إضافة الفقرة السابقة هو حماية المعلومات وأنظمة الحاسبات الآلية من أعمال الإتلاف التي ترتكب بواسطة أشخاص غير مصرح لهم بالدخول إلى النظام وذلك في حالتين: الأولى إذا ترتب على الإتلاف خسائر مادية تقدر بألف دولار أو أكثر خلال العام الواحد، والثانية أن تمس أعمال الإتلاف معلومات طبية، وفي هذه الحالة الأخيرة لا يؤخذ في الاعتبار الخسائر المادية الناجمة عن الإتلاف.

وفي عام 1996م صدر قانون حماية بنية المعلومات القومية The NII Protection Act وبصدوره عدلت المادة السابقة 1030- أ حيث تم التوسيع من نطاق حماية أنظمة الحاسبات الآلية، حيث لم تعد الحماية قاصرة على الحاسبات الآلية التابعة للحكومة وإدارتها أو التي تستخدم من قبلها أو لصالحها، وإنما اتسعت الحماية لتشمل جميع الحاسبات التي يتم استخدامها من قبل المؤسسات الاقتصادية التابعة لحكومة الولايات المتحدة

الأمريكية، وكذلك تلك التي تستخدم في التجارة والاتصالات بين الولايات الأمريكية فيما بينها أو بين الولايات الأمريكية والدول الأخرى، وهو ما أطلق عليه الحاسبات الآلية التي تتمتع بالحماية، كما امتد النص ليشمل أعمال الإتلاف التي تقع من أشخاص مصرح لهم بالدخول إلى النظام متى ما تم ذلك عمدًا.

ومن أهم ما أتت به المادة 1030-أ بعد تعديلها تجريم الإتلاف المعلوماتى، فالبند الأول من الفقرة الخامسة ينص على "تعديل المعلومات والبرامج والشفرات والأوامر داخل أنظمة الحاسبات الآلية، مما يترتب عليه أضرار تلحق بحاسب آلي يتمتع بالحماية متى ما كان إحداث الضرر قد تم عمدًا." والفعل الإجرامي هنا يعد جناية[1].

ويتضح من العرض السابق أن موقف المشرع الفرنسي يتسم بالبساطة والمنطق، فلم يغرق في التفاصيل كما فعل المشرع الأمريكي، حيث نص على الجرائم دون أن يحدد الجهة التي يتبع لها نظام معالجة البيانات[2].

(1) انظر حول ذلك: - د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, مرجع سابق, ص 425, د. نائلة عادل محمد فريد, جرائم الحاسب الاقتصادية, مرجع سابق, ص 219.

- Heymann (Stephen p), Legislating Compyter Crime, H.J.L, 1997, vol.34.

- http://www.startimes2.com/f.aspx

(2) صدر في الولايات المتحدة الأمريكية القانون الفيدرالي في شأن الاعتداء على الكمبيوتر واستغلاله في عام 1984، وعدل في أعوام 1986، 1994، 1996، وورد في الفصل (1030) منه نصوص خاصة تجرم الاعتداء على الكمبيوتر والمتعلقة بأنشطة متصلة بالكمبيوتر، وقد تبين بعد ذلك أن القانون ينطوي على الكثير من الغموض والقصور، بحيث يمكن للمجرمين أن يتلافوا تطبيق القانون عليهم باستخدام حاسبات وشبكات تقع خارج الولايات المتحدة الأمريكية، كما يمكن لمجرمي الكمبيوتر من خارج الولايات المتحدة الأمريكية استخدام الأنظمة =

أما اتفاقية بودابست الأوروبية فقد جرمت الإتلاف الذي تتعرض له المكونات المنطقية للحاسب الآلي، ونصت على عدة صور يتم بها الإتلاف المعلوماتي كالإلغاء والإفساد والتدمير وغيرها، حيث نصت في الفقرة الأولى من المادة 4 على أنه: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية للتجريم تبعًا لقانونه المحلي إذا أحدث ذلك عمدًا ودون وجه حق, أي إضرار أو محو, أو تعطيل, أو إتلاف, أو طمس لبيانات الحاسب.

والهدف من وراء تقرير هذا النص كما أشارت المذكرة التفسيرية لهذه الاتفاقية هو ضمان حماية مماثلة للبيانات والبرامج المعلوماتية كتلك التي تتمتع بها الممتلكات المادية ضد الخسائر والأضرار التي تحدث لها عن عمد, والمصالح القانونية المحمية هي سلامة وحسن تشغيل أو حسن استخدام البيانات أو برامج الحاسب المسجلة[1].

وفي النهاية نرى أن قانون مكافحة جرائم تقنية المعلومات الإماراتي، والقانون الجنائي الفرنسي يحققان حماية متكاملة لأجهزة الحاسب الآلي وبرامجها ضد الإتلاف، وسواء أكانت أموالا مادية أو معنوية[2]، وذلك

= الموجودة بالدولة للاعتداء على حاسبات تقع في دول أخرى, راجع حول ذلك د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 41 وما بعدها.

(1) انظر حول ذلك: د. هلالي عبد اللاه أحمد, اتفاقية بودابست لمكافحة جرائم المعلوماتية, مرجع سابق, ص 68, د. عمر محمد بن يونس, الاتفاقية الأوروبية حول الجريمة الافتراضية, مرجع سابق, ص 74.

(2) د محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 188.

بتحديدهما بدقة صور الإتلاف، ففي القانون الفرنسي هي[1] المحو الإلكتروني للبيانات بتدميرها كلها أو جزء منها، وإدخال بيانات في نظم المعالجة الآلية لم تكن موجودة من قبل، مما يؤدي إلى التشويش على صحة البيانات القائمة، وتعديل البيانات بتعديل طرق انتقالها ووسائل هذا الانتقال، وتعطيل أو إفساد تشغيل النظام، وقد توسع القانون الإماراتي في هذه الصور، فنص على الإلغاء أو الحذف أو التدمير أو الإفشاء أو الإتلاف أو التغيير، بجانب إعادة نشر البيانات أو المعلومات.

كما أن هذه الحماية تتوافق مع الاعتبارات العلمية والعملية في الاعتراف للبرامج والمعلومات بصفة المال وهو اعتراف له ما يبرره من الناحية العملية، فبرامج الكمبيوتر كيان غير مادي يمكن رؤيته على شاشة الحاسب، ويمكن ترجمته إلى أفكار، وبالتالي فله مصدر وله مالك، ويمكن الاستحواذ والسيطرة عليه عن طريق تشغيله في الحاسب الآلي، وهو ما جعل المشرع الفرنسي يعترف بأن لفظ الأشياء يشمل الأشياء المادية والمعنوية، كما أن الرأي المخالف لا يواكب التطور التكنولوجي، ولا يحاول التحرر من المفهوم التقليدي لتعريف المال، كما أن عدم الاعتراف بصفة المال للمعلومات والبرامج من شأنه أن يحرمها من الحماية الجنائية.[2]

والاعتداء على البيانات إما أن يتم بمحو تلك البيانات والمعلومات كلية وتدميرها إلكترونيًا، أو أن يتم بتشويه المعلومة أو البرنامج عن طريق

(1) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 49.
(2) د. هدى حامد قشقوش، الإتلاف العمدي لبرامج وبيانات الحاسب الإلكتروني، مرجع سابق، ص11.

تعديل البيانات، أو تعديل طرق معالجتها أو وسائل انتقالها، إضافة إلى الصور الواردة في المادة والمتمثلة في الإفشاء أو إعادة نشر هذه البيانات.

وإتلاف البيانات قد يثير اختلافًا من ناحية تكييفها القانوني بحسب الغاية التي هدف إليها المجرم المعلوماتي من واقعة الإتلاف، إذ قد يشكل الفعل إتلافا بالمعنى القانوني إذا كانت هذه المعلومات والبرامج محل الإتلاف هي هدف الجاني، أي دون أن تتجه إرادته لارتكاب جريمة أخرى، وقد تكون بعض الأفعال الإجرامية مكيفة بتكييف معين على الرغم من وجود تكييف آخر لها، ومن التطبيقات القضائية تكييف واقعة قيام محاسب بمحو بيانات ومعلومات معالجة آليًا تخص إحدى الشركات على أنها تشكل جريمة نصب معلوماتي؛ إذ اعتبر المحو الذي وقع بالاعتداء على البيانات الموجودة بالبرنامج يشكل جريمة نصب على الرغم من أن المحو من وسائل الإتلاف، وكذلك قد يكيف الاعتداء بتغيير أو تعديل بيانات إلكترونية على أنه يشكل جريمة تزوير، وقد تكيف الطلبات المزورة أيضًا التي تحدث عن طريق الشركات في طلب البضائع بالتلاعب مع الشركات بتعديل المعلومات على أنها اختلاس أموال.[1]

الفرع الثاني

القصد الجنائي في جريمة الإتلاف

الإتلاف من الجرائم العمدية، ويتحقق متى تعمد الجاني ارتكاب الفعل المنهي عنه بالصورة التي حددها القانون، واتجاه إرادته إلى إحداث الفعل وبأي صورة من الصور التي أوردها قانون مكافحة جرائم تقنية المعلومات،

(1) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، عمان، 2004، ص 230.

وهي في قانون العقوبات الفرنسي: المحو الإلكتروني للبيانات بتدميرها كلها أو جزء منها، أو إدخال بيانات في نظم المعالجة الآلية لم تكن موجودة من قبل، مما يؤدي إلى التشويش على صحة البيانات القائمة، أو تعديل البيانات أي تعديل طرق انتقالها ووسائل هذا الانتقال، أو تعطيل أو إفساد تشغيل النظام، مع علمه بأنه يقوم بفعله الإجرامي بغير حق على مال مملوك لغيره.

وهي في القانون الإماراتي تتم بإلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو إعادة نشر بيانات أو معلومات.

والسؤال الذي يطرح نفسه هو عن مدى تحقق جريمة الإتلاف إذا ما وقعت بطريق الخطأ، وللإجابة نجد أن نص قانون مكافحة جرائم تقنية المعلومات الإماراتي، ونص قانون العقوبات الفرنسي جاءا خاليين من الإجابة على هذا السؤال.

ولكن وبالعودة للنص التقليدي المنصوص عليه في المادة 424 في قانون العقوبات الإماراتي، واستنادًا إلى المادة 43 من القانون ذاته والتي نصت على أن: "يسأل الجاني عن الجريمة سواء ارتكبها عمدًا أو خطأ، ما لم يشترط القانون العمد صراحة". ولقد قضت محكمة التمييز في دبي بأن للقاضي الجزائي تقرير ركن الخطأ والتقصير في التسبيب في إلحاق الضرر بالمال، وحسبه أن يقيم قضاءه على أسباب سائغة لها أصلها الثابت في الأوراق وكافية لحمله، فيكفي لقيام الجريمة صدور الهدم أو الإتلاف لمال الغير عمدًا أو خطأ.[1]

ووفقًا لأحكام محكمة النقض المصرية فإن جريمة الإتلاف إنما هي جريمة عمدية يتحقق القصد الجنائي فيها متى تعمد الجاني ارتكاب الفعل

(1) الطعن رقم 1993/28 (جزاء) جلسة السبت 23 /1993/10، محكمة تمييز دبي.

المنهي عنه بالصورة التي حددها القانون، واتجاه إرادته إلى إحداث الإتلاف أو التخريب، وعلمه بأنه يحدث الفعل المادي المكون للجريمة بدون وجه حق، فإذ لم يستظهر الحكم القصد الجنائي في جريمة الإتلاف وكانت مدوناته لا تفيد في ذاتها أن الطاعن قد تعمد إتلاف المنقولات موضوع الاتهام، فإن الحكم المطعون فيه يكون مشوبًا بالقصور في التسبيب.[1]

المطلب الثاني

الإتلاف المعلوماتي وحماية التجارة الإلكترونية

يؤدي تجريم الإتلاف العمدي للمال المعلوماتي بالضرورة إلى ضرورة حماية نظم معالجة البيانات، ومنها تلك التي تتعلق بالتجارة الإلكترونية عبر شبكة الإنترنت، والتي تعتمد على مجموعة برامج وبيانات ومعلومات تبث عبر الشبكة، وتمثل المواقع التي يتم فيها الإعلان عن السلعة أو الخدمة، وطريقة أداء مقابل الوفاء عند التعاقد، وتأمين الاتصال ما بين العملاء سواء بين المنتج والمستهلك أو البائع والمشتري، تمثل هذه المواقع المحور الرئيسي لعملية التجارة الإلكترونية، ومما لا شك فيه أن إتلاف هذه المواقع سوف يؤدي بالضرورة إلى خسائر مادية جسيمة بالنسبة للشركات والمستهلكين الذين يعتمدون على التجارة الإلكترونية فضلا عن ضعف ثقة العملاء بها، ونتناول في هذا المطلب طرق الإتلاف، والحماية التشريعية لمواقع التجارة الإلكترونية كلٌّ في فرع كالآتي.

---

(1) طعن رقم 2824 لسنة 56 قضائية، جلسة 1986/10/9، نقض مصري جنائي.

الفرع الأول

وسائل الإتلاف المعلوماتي

يتحقق الإتلاف المعلوماتي للبرامج والمعطيات عن طريق استعمال الفيروس أيًا كان أثره، مادام كان من شأن ذلك أن يؤدي إلى اضطراب في عمل الكمبيوتر، فلا يلزم في الفيروس أن يكون من شأنه مسح جميع المعلومات أو جزء منها، بل يسري نص التجريم على كل برنامج يسبب خللا في نظام عمل الكمبيوتر، ويعد من قبيل هذا الخلل البطء في سير الجهاز أو تقليل كفاءته[1]، والحقيقة أن الفيروس يؤدي إلى إبطاء البرامج الخاصة بنظام التشغيل أو البرامج الخاصة بالمعالجة، مما يؤدي إلى شغل ذاكرة الجهاز أو الأسطوانة كاملة في لحظة من اللحظات، وبالتالي يكون من المتعذر التعامل مع هذه المعطيات أو المعلومات سواء بمعالجتها أو باستخدامها مطبوعة على أوراق، لأن البرنامج لا يستجيب لأي تعليمات توجه إليه، وذلك لعدم وجود سعة أو فراغ في ذاكرة الحاسب الآلي، وبالتالي تفقد كل المعلومات المخزنة بالجهاز أو المسجلة على الأسطوانة فائدتها، ولا يمكن حذف جزء منها مع عدم الاستجابة لأوامر التشغيل وتوقف النظام، فيصبح عديم الجدوى[2].

ويتولى إعداد هذه الفيروسات ونشرها فئة من خبراء الحاسب الآلي قد يكون هدفهم إثبات الذات أو الدعاية أو مجرد إيذاء الآخرين[3]، وقد تتهم في

(1) د. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق، ص 20.

(2) د. مدحت عبد الحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت، مرجع سابق، ص 50.

(3) د. عبد الفتاح بيومي حجازي، الحماية القانونية للتجارة الإلكترونية، دار الفكر =

ذلك بعض الشركات الكبرى التي تقوم بإنتاج هذه البرامج حماية لبرامجها، حيث تنطلق الفيروسات عند محاولة النقل غير المشروع.[1]

وفيروس الكمبيوتر هو مرض يصيب الجهاز، وهو عبارة عن برنامج صغير يمكن تسجيله أو زراعته على الأسطوانات المرنة أو الأقراص الصلبة الخاصة بالحاسب، ويظل هذا الفيروس خاملا خلال فترة محدودة، ثم ينشط فجأة في توقيت معين ليدمر البرامج والمعلومات المسجلة في الحاسب، الأمر الذي يؤدي إلى إتلاف المعلومات أو حذفها أو تدميرها[2]، ومن المعروف أن فيروسات الكمبيوتر هي برمجيات من صنع وتصميم البرمجيين.[3]

= الجامعي، الإسكندرية، 2002، ص 120، ويرى أن اختراق الشبكات والفيروس المعلوماتي ينظر إليها بوصفها من مشكلات التجارة الإلكترونية، وفي المعنى ذاته د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص 101.

(1) ففي ألمانيا أدين مهندس يعمل لدى إحدى المنشآت لتسببه في محو برامج على نحو غير مشروع لمجرد رغبته في جذب نظر العامة إليه، وفي فرنسا حامت الشبهات حول منافسين لأسواق (hpermarch) لتورطهم في إدخال نوع من الفيروسات إلى البرامج بقسم السلع، أدى إلى قصور في مخازن هذه الأسواق وانخفاضها بشكل غير حقيقي، الأمر الذي تسبب في خسارة قدرها (11) مليون فرنك فرنسي، بالإضافة إلى عمل متواصل لمدة شهر لإعادة الحال إلى ما كان عليه.
راجع في ذلك د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 190، وكذلك هامش ص 191.

(2) د. جميل عبد الباقي الصغير، مقدمة في الحاسب الآلي، (دراسة عملية ونظرية)، دار النهضة العربية، القاهرة، 1999 / 2000، ص 178.

(3) د. محسن محمد العبودي، كارثة فيروسات الكمبيوتر والجرائم المتعلقة بالإنترنت، بحث منشور على شبكة الإنترنت www.arablawinfo.com ص 17.

كما تم تعريفه بأنه برنامج حاسب مثل أي برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدد، وهو إحداث أكبر ضرر ممكن بنظام الحاسب، ولتنفيذ ذلك يتم إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيًا وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في الذاكرة حتى يحقق أهدافه التدميرية.[1]

والفيروس عبارة عن برنامج يتميز بثلاث خواص هي التضاعف, والتخفي, وإلحاق الأذى بالآخرين, ويتمثل النشاط التدميري له في أنه يقوم بمسح البيانات والمعلومات المخزنة على وسائط التخزين وإتلافها، لذا يطلق على هذه العملية اسم مسح البيانات وتحويلها إلى صفر Zeroing[2].

ويصعب تحديد البداية الفعلية لظهور أول فيروس، وإن كان من المرجح أن أول ظهور لفيروس كان في عام 1978 وهو الفيروس المسمى [المخ Brain] والذي اقتحم 350 ألفًا من حاسبات IBM والحاسبات المتوافقة معها، واعتمدت الفيروسات الأولى في انتشارها على الأقراص المرنة التي تحتوي برامج منسوخة، أما الآن فالبريد الإلكتروني وشبكة الإنترنت هي المصدر الرئيسي للفيروسات[3].

---

(1) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2003، ص 26، وراجع حول ذلك د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات, مرجع سابق، ص 163، ود. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 189، ود. محمد علي العريان، الجرائم المعلوماتية، مرجع سابق، ص 83.

(2) د. عبادة أحمد عبادة, التدمير المتعمد لأنظمة المعلومات الإلكترونية, منشورات مركز البحوث والدراسات, شرطة دبي, مارس 1999, ص 1.

(3) http: www et. 8m. com / virusty pes. Htm

من أشهر حوادث الفيروسات ما جرى في الثالث من نوفمبر في عام 1988 حين تمكن طالب جامعي أمريكي من إدخال فيروس الدودة إلى شبكة الإنترنت من خلال إحدى وسائل الاتصال، وفي مدة لا تتجاوز 24 ساعة كان هذا البرنامج قد انتشر عبر الشبكة وغطى أطرافها كلية، وتأثرت به شبكات كبيرة ترتبط بشبكة الإنترنت، وتقدر بأكثر من 6000 حاسب في أرجاء الولايات المتحدة الأمريكية، حيث قام هذا الفيروس بملء ذاكرتها حتى لم يعد بمقدورها القيام بأي عمل أو تنفيذ أي أمر، مما شكل إتلافا للمعلومات[1].

وفي واقعة أخرى اعتقلت شرطة ولاية نيوجرسي في الولايات المتحدة المتهم [ديفيد سميث] الذي أنشأ فيروس البريد الإلكتروني المعروف باسم [ميلسا] الذي أحدث اضطرابًا عالميًا في البريد الإلكتروني وشبكة الإنترنت[2].

ومن أبرز الهجمات الفيروسية التي شهدها عالم الحاسبات والمعلوماتية اقتحام الفيروس الباكستاني (Pakistani Virus) المعروف أيضًا باسم المخ أو الدماغ (Brain) لحوالي 350 ألف من حاسبات أي بي إم والحاسبات المتوافقة معها.[3]

---

(1) سبق الحديث عن هذا الطالب وهو موريس (Morris)، 23 عاما، من جامعة كورنل، وقد ابتكر برنامجا يمكنه من إعادة طبع أو تكرار ذاته وإعادة بث ذاته، ومهمته الاختراق، وأطلق عليه تسمية الدودة، وكانت النتائج السلبية مذهلة بعد إطلاقه، وتم إدانته من قبل القضاء الأمريكي بالوضع تحت المراقبة لمدة (3) سنوات، وكذلك أربعمائة ساعة في العمل الاجتماعي.

(2) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 49.

(3) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 168.

والحقيقة أن أغلب النصوص التشريعية لم ترقَ بعدُ إلى الحد الذي تجرم هذه الأعمال وحيازة وإعداد البرامج والأنظمة الخاصة بإعداد الفيروسات والبرامج الخبيثة والمدمرة والتي تؤدي إلى إتلاف الأجهزة والبرامج.

والفيروس قد يستهدف برنامج الحاسب، أو البيانات المخزنة فيه، فيقوم بالتحرك من ملف لآخر، والحصول على معلومات وبيانات، والقيام بحذف أو تعديل أو استبدال هذه البيانات.

وتمتاز الفيروسات بعدة مزايا، كالقدرة على الاختفاء عن المستخدم فلا يلاحظها إلا بعد أن تصيب الجهاز؛ حيث تتمركز في أماكن معينة يصعب على المستخدم وخاصة غير المتخصص ملاحظتها مثل الذاكرة، وتنتظر في هذا المكان حتى تشير الساعة إلى تاريخ معين فتقوم بتشغيل نفسها وتنفيذ أعمالها التدميرية.[1]

كما تمتاز الفيروسات بمجموعة من الخصائص التي تؤمن لها القيام بدورها التخريبي والمعطل، ومنها:

1) القدرة على التخفي: للفيروسات قدرة كبيرة على التخفي والخداع عن طريق الارتباط ببرامج أخرى للتمويه، كالدخول إلى ملفات مخفية أو الخاصة بالذاكرة، وبعد فترة معينة أو مباشرة يشغل نفسه ويبدأ نشاطه التدميري.

2) القدرة على العدوى: حيث يزرع الفيروس على الأسطوانات الخاصة بالحاسب، وبمجرد تحميله ينتقل وينسخ نفسه من ملف لآخر بسرعة كبيرة.

3) الاختراق: يتمتع الفيروس بقدرة فائقة على الدخول للنظام والتسلل إليه واختراق سبل الحماية.

(1) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 28.

4) التدمير: الهدف الأساسي للفيروسات هو تخريب وتعطيل البرامج، وأهم مظاهرها إبطاء جهاز التشغيل.[1]

ويمكن التمييز بين الفيروسات وبرامج التجسس، فبرامج التجسس غير مصممة لتدمير جهاز الحاسوب، بل إنها تدخل دون إذن وتختفي في الخلفية بينما يحدث تغييرات غير مرغوب بها للمستخدم، وتتسبب برامج التجسس في تدمير الملفات أكثر من إنتاجها، وهي تنتقل عند ارتكاب خطأ ما من قبل المستخدم كالضغط على أحد أزرار النوافذ الخاصة بنقل البرامج التجسسية، أو تحميل البرامج غير الآمنة عبر مواقع شبكة الإنترنت.

وللفيروس أهداف متعددة يقصدها مصممه أو مبرمجه من إنشائه وبثه ومنها:

1) قد يقوم القرصان بإنشاء الفيروس لإثبات ذاته ورغبة في التحدي وإبراز المقدرة الفكرية من بعض الأشخاص الذين يسخرون ذكاءهم وقدراتهم بشكل سيء.

2) بهدف عدواني للاطلاع على إمكانية الغير المنافس وإضعافها، وتكبيده خسائر مالية ضخمة في القطاع السياسي أو العسكري أو الاقتصادي.

3) لابتزاز الشركات الكبرى والبنوك، كما أن الشركات التجارية الكبرى تعيش فيما بينها حربًا اقتصادية قد تستغل فيها نظام الفيروسات.

4) الرغبة في الانتقام من قبل بعض المبرمجين المطرودين من أعمالهم والناقمين على شركاتهم، وتصمم الفيروسات في هذه الحالة بحيث تنشط بعد تركهم العمل بفترة كافية، أي تتضمن قنبلة منطقية موقوتة.

5) التشجيع على شراء البرامج المضادة للفيروسات، إذ تقوم بعض

(1) د. محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2003، ص 294.

شركات البرمجة بنشر فيروسات جديدة ثم تعلن عن منتج جديد لكشفها.

6) التسريح من العمل: فقد يقوم العمال بالاعتداء على المؤسسات التي يعملون بها بسبب تسريحهم من العمل.[1]

7) الدافع السياسي والعسكري: مما لا شك فيه أن التطور العلمي والتقني أديَا إلى الاعتماد على أنظمة الكمبيوتر في أغلب الاحتياجات التقنية والمعلوماتية، خاصة في الميادين العسكرية والحربية، الأمر الذي يعتبر الدافع نحو تشجيع الدول إلى استخدام مثل هذا السلاح.

ومن ناحية أخرى فإن للفيروسات أهدافًا قد تعتبر مشروعة في بعض الأحيان من وجهة نظر مصنعها، كحماية النسخ الأصلية للبرنامج من النسخ غير الشرعي، حيث ينشط الفيروس بمجرد النسخ وذلك من أجل حماية هذه البرامج، كما قد يسلم البرنامج مع الفيروس ليقوم الأخير بتدمير البرنامج وذاكرة الحاسب إذا لم يف العميل بالتزاماته، وإذا ما وفى يقوم المنتج بإبطال مفعول الفيروس.[2]

والفيروسات التي تصيب الحاسب الآلي متعددة، ويمكن تقسيمها من حيث تكوينها وأهدافها إلى ما يلي[3]:

أ) فيروس عام العدوى: وهو يصيب أي برنامج أو ملف.

(1) هناك محترفون في القرصنة تم القبض عليهم بالولايات المتحدة، وبعد التفاوض معهم تم تعيينهم بوكالة المخابرات الأمريكية (CIA) ومكتب التحقيقات الفيدرالية (FBI) وتركزت معظم مهماتهم في مطاردة الهاكرز وتحديد مواقعهم لإرشاد الشرطة إليهم.

(2) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، مرجع سابق، ص 238.

(3) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 191.

ب) فيروس محدد العدوى: وهو يصيب نوعًا معينًا من النظم، ويتميز عن سابقه بالبطء في الانتشار وصعوبة اكتشافه.

ج) فيروس عام الهدف: يمتاز بسهولة إعداده واتساع مدى تدميره، والغالبية العظمى من الفيروسات تندرج تحته.

د) فيروس محدد الهدف: وهذا النوع من الفيروسات يقوم بتغيير الهدف من عمل البرنامج دون أن يعطله، ويحتاج إلى مهارة عالية في التطبيق المستهدف، كأن يحدث تلاعبًا ماليًا أو تعديلا معينًا في تطبيق عسكري.

أما من حيث الأضرار التي تحدثها الفيروسات بأجهزة الكمبيوتر فتنقسم إلى عدة أنواع[1]:

1) فيروسات قطاع التشغيل: وهي من أخطر أنواع الفيروسات إذ يقوم بزرع نفسه في قطاع التشغيل أو الإقلاع مما يمنعك من تشغيل الجهاز.

2) فيروسات الملفات: وتسمى أيضًا بفيروسات البرامج، وهي تربط نفسها بالتطبيقات والملفات التنفيذية، وهي تتكاثر بتنشيط التطبيق المصاب وتقوم بإصابة ملفات جديدة.

3) الفيروسات المتعددة: وهي تصيب كلا من قطاع التشغيل والملفات، وهذا ما يجعلها أسرع أنواع الفيروسات في التكاثر.

4) الفيروسات الطفيلية: هي تلك الفيروسات التي تربط نفسها ببعض الملفات حتى تتكاثر، وهي تضيف عدة سطور للملف التنفيذي المصاب، فكلما عمل هذا الملف عمل الفيروس وبدأ بالتكاثر.

5) الفيروسات المرافقة: وهذه لا تهاجم إلا الملفات التنفيذية، وهي تعتمد

---

(1) http:// wwweb. 8m.com/virustypes.htm

على ميكانيكية معينة بتخليق ملف com وهو يرافق الملف التنفيذي في التشغيل، فكلما عمل الملف التنفيذي عمل الملف الملوث بالفيروس.

6) الفيروسات الاستبدالية: عندما يعمل الفيروس يبحث عن ملف غير مصاب ويستبدله بملف ملوث من نفس الحجم ويدمر الملف الأصلي، لذا يبدو وكأنه يعمل ولكنه في الحقيقة لا يفعل شيئًا.

7) فيروس الماكرو: وهو عبارة عن ماكرو خبيث تم كتابته لأغراض تدميرية، وهو يؤثر على برامج مايكروسوفت أوفيس مثل وورد وإكسل وهو غالبًا يعدل الأمر (حفظ) ليشغل نفسه بعد ذلك تلقائيًا.

8) الفيروسات المتحولة: وهي تلك الفيروسات التي تتبدل أوامرها كلما انتقلت من جهاز إلى آخر، ولكنها في العادة تكون مكتوبة برداءة شديدة تمنعها من الانتشار مما يسهل إزالتها.

ومن أشهر الفيروسات التي تم اكتشافها والتعامل معها هي:

1) فيروس مايكل أنجلو: ظهر هذا الفيروس في 26 مارس 1992 بمناسبة الاحتفال بذكرى ميلاد الرسام الإيطالي الشهير مايكل أنجلو، ويقوم بمسح معلومات القرص الصلب للأجهزة المصابة به.

2) فيروس ناسا: وأطلق هذا الفيروس احتجاجا على نتائج الأسلحة النووية، وكان هدفه اختراق الحاسب الآلي لوكالة الفضاء الأمريكية (ناسا).

3) فيروس الكريسماس: ويتمثل في صورة رسالة ترسل إلى أحد الأشخاص كتهنئة بمناسبة أعياد الكريسماس، وفي الوقت نفسه تقوم بقراءة عناوين المشتركين في البريد الإلكتروني، ثم ترسل هذه الرسالة إلى تلك العناوين، الأمر الذي يترتب عليه أن يتوقف النظام

بأكمله لحين القضاء على هذا الفيروس[1].

4) فيروس الحب: الذي خرج من الفلبين في 4 مايو 2000 وهو ليس معقدًا من الناحية الفنية مقارنة بفيروس مليسا [Melisa] والذي اجتاح العالم، ولكنه أسرع منه بمراحل في الانتشار، وانتشر فيروس الحب من خلال أنظمة الرسائل الفورية التي تتيح لمستخدمي شبكة الإنترنت التخاطب مباشرة مع بعضهم البعض، واستهدف هذا الفيروس أساسًا أجهزة الكمبيوتر التي تعمل بنظام ويندوز الذي تنتجه شركة مايكروسوفت العملاقة، والتي تستخدم نظام إكسبلورر لتصفح شبكة الإنترنت، وظهور الفيروس في البريد الإلكتروني على صورة رسالة بعنوان [أحبك] [I Love You] وفي حالة فتحها ينتشر الفيروس في جميع العناوين المسجلة لدى مستخدمي البريد الإلكتروني في أجهزة الكمبيوتر الأخرى، ثم يتسلل إلى جهاز الكمبيوتر ليدمر محتوياته[2].

5) فيروس تشيرنوبيل: فقد كانت كارثة المفاعل النووي الروسي في أوكرانيا في 26 من أبريل عام 1986 هي الحافز وراء برمجة فيروس سمي بنفس الاسم، وينشط للعمل في نفس التاريخ من كل عام، ويؤكد الخبراء على أن فيروس تشيرنوبيل بالغ الدقة، ينتقل عبر شبكة الإنترنت فيتسلل إلى أجهزة الكمبيوتر، حيث يدمر المعلومات المخزنة ويلغي الملفات الموجودة في الذاكرة، بل يضغط على القرص الصلب

---

(1) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة، دراسة مقارنة، جامعة الإسكندرية، 2000، ص 204.

(2) http:// www.islamonline. net/ iol.arabic/dowalia/scince.14/ scincel. Asp

مما يؤدي في حالات كثيرة إلى إتلاف تلك الرقائق وتدميرها، وقد أمكن تلافي أخطار هذا الفيروس بطريقة بسيطة جدًّا، وذلك بتغيير تاريخ نشاطه ثم إعادة تصويب التاريخ مرة أخرى مع العديد من الفيروسات المؤقتة[1].

وبالإضافة إلى ما سبق هناك ما يعرف باسم البرامج الخبيثة، وهي ليست فيروسات بالمعنى الحرفي، ولكنها مصممة في الأساس لإلحاق الضرر بالمستخدم ومنها:

- الديدان:

وهو برنامج تمت كتابته بغرض الانتشار بين شبكة من الكمبيوترات، وهو بعكس الفيروسات لا تحتاج لبرنامج وسيط لكي تتكاثر، وأيضا تحاول إصابة أجهزة الحاسب الأخرى، وغالبًا فإن ضررها الأساسي في إبطاء سرعة عمل الشبكات.

- أحصنة طروادة:

تمامًا مثل الأسطورة القديمة عندما اختفى الجنود داخل الحصان الخشبي ليدخلوا طروادة ويهزموا أهلها، هكذا فإن أحصنة طروادة هي برامج خبيثة تختفي بداخل برامج مفيدة، وغرضها الأساسي هو جمع المعلومات مثل الاسم وكلمة السر، ثم يبعث البرنامج بهذه المعلومات لصاحبه أثناء اتصال الجهاز بالشبكة، والأسوأ من ذلك أنه سيسمح للهاكر بتصفح جهازك أو التحكم بملفاتك تحكمًا كاملا.

- التحذيرات المضللة:

وهي عبارة عن رسائل إلكترونية كتبت بعناية بهدف إشاعة تحذيرات

---

(1) http://www.islamonline.net/iol،arabic/dowalia/scince،14/dcincel.asp

مضللة هدفها في الأصل بث الرعب بين المستخدمين، وهي في العادة يكون موضوعها عن تهديدات وهمية، والشيء المميز لهذه الرسائل أنها تطلب منك أن ترسل هذه الرسائل إلى أكبر قدر من الناس المقربين لك لتحذيرهم، ولا يجب إرسالها لأن هذه هي الطريقة التي تعتمد عليها التحذيرات المضللة في الانتشار[1].

هذه أمثلة لبعض الفيروسات، وهناك الكثير غيرها والتي تنتشر بسرعة مذهلة عبر شبكة الإنترنت متخطية حدود الزمان والمكان، ويتم في بعض الأحيان القبض على ناشري تلك الفيروسات ومصنعيها مثلما تم القبض على الفتى الفلبيني الذي نشر فيروس الحب، وكذلك ما جرى مؤخرًا من محاكمة البريطاني العاطل عن العمل [كريستو فربابل] في بريطانيا بعد أن ثبتت عليه تهمة قيامه بتطوير فيروس الحاسب الآلي (كوييج Kuig) و(باتوجين Batogine)، بالإضافة إلى قيامه بإصدار دليل علمي يساعد المبرمجين على تطوير فيروسات خاصة بهم، وقد حوكم (بابل) بالاستناد إلى قانون إساءة استعمال الحاسب الآلي الصادر سنة1990[2].

ويقدر الخبراء أن هناك ما يقارب 86 ألف فيروس معروف، ونحو 700 فيروس آخر يجري تصميمه كل أسبوع.[3]

والجدير بالذكر أن قانون مكافحة جرائم تقنية المعلومات الإماراتي نص في المادة (6) على أنه: "كل من أدخل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، ما من شأنه إيقافها عن العمل أو تعطيلها، أو

(1) wwweb. Fm. Com/ virustypes. htm

(2) http:// www.islamonline. net/ iol،arabic/dowalia/scince،14/ scincel. Asp

(3)http://news.bbc.co.uk/hi/arabic/sci،tech/newsid،3359000/3359369.stm

تدمير أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات فيها، يعاقب بالسجن المؤقت، وبالغرامة التي لا تقل عن خمسين ألف درهم، أو بإحدى هاتين العقوبتين".

فهذه المادة تتصدى لكل من يبث الفيروسات والبرامج الخبيثة عن طريق الشبكة المعلوماتية أو عن طريق أية تقنية من تقنية المعلومات، ويكون من شأن هذه البرامج أن تؤدي إلى الإتلاف بمختلف صوره كأن تؤدي إلى إيقاف الشبكة عن العمل أو تعطيلها أو تدميرها، أو مسح أو حذف أو إتلاف أو تعديل البرامج أو البيانات أو المعلومات.

ولكن المشرع لم يحدد عقوبة لمن يقوم بإعداد هذه البرامج أو ترويجها، ولكن الملاحظ أن عقوبة هذه المادة هي السجن، وبالتالي فالجريمة هنا جناية، والشروع مفترض فيها، وبالتالي من الممكن معاقبة المتهم بحيازة هذه البرامج بجريمة الشروع في بثها إذا بدأ في أي ركن من أركان الجريمة، ولكن مجرد الحيازة المجردة فإنها تدخل في الأعمال التحضيرية غير المجرمة.

مما سبق يتضح لنا أن إنشاء الفيروسات يؤثر على أنظمة المعلومات، فالمعلومة هي المادة الخام للبرامج وقواعد البيانات؛ ومتى ما صيغت بأسلوب إبداعي فيه ابتكار في الأنشطة الصناعية أو التجارية فإنه يدخل في نطاق الحماية القانونية، والفيروسات تشكل في حد ذاتها اعتداءً على البرامج وقواعد البيانات وأنظمة المعلومات، لكونها تعمل على تخريب وتعطيل هذه البرامج والاعتداء عليها.[1]

---

(1) د. أمجد حسان، الفيروسات إرهابا تهدد أنظمة المعلومات، مقال مقدم إلى ملتقى الإرهاب في العصر الرقمي، جامعة الحسين بن طلال، عمان، 10 - 12 يوليو 2007، ص 21. ومتوفر على العنوان التالي:

=

الفرع الثاني

الحماية التشريعية لمواقع التجارة الإلكترونية

تتمثل الحماية التشريعية لمواقع التجارة الإلكترونية في ضرورة إعداد التشريعات الملائمة التي تضمن عدم إفلات الجاني الذي يتسبب في خسائر فادحة من جراء قيامه بإتلاف وتدمير مواقع هذه التجارة الإلكترونية مستندًا إلى عدم وجود نص عقابي ينطبق عليه[1]، وهو ما سبق لنا بيانه في الفرع الأول من خلال عرض موقف التشريع الإماراتي والمصري والفرنسي- من جريمة الإتلاف العمدي، وهو الموقف الذي ينطبق على تشريعات غالبية الدول التي لم تجد في قوانينها العقابية القائمة القدرة على بسط الحماية الجنائية للأموال المتداولة عبر الوسائط الإلكترونية، ومنها تلك التي تتعلق بالتجارة الإلكترونية، وذلك من خلال تجريم الاعتداء على الأموال المعلوماتية، وهو ما أدى إلى أن سارعت هذه الدول وعدلت تشريعاتها العقابية وأصدرت تشريعات جديدة لمواجهة النماذج الجديدة من الإجرام المعلوماتي، ومنها بالطبع جرائم الأموال متى وقعت بطريق معلوماتي، ومن هذه الدول فرنسا والولايات المتحدة وكندا وألمانيا ومعظم دول غرب أوروبا، والإمارات العربية المتحدة، والمملكة العربية السعودية، والمملكة المغربية.

وأكثر من هذا فإن القوانين المعلوماتية الجديدة في بعض هذه الدول حاولت التحرر من المبادئ التقليدية الموضوعية والإجرائية التي تحكم القوانين الجزائية، مثل مبدأ المشروعية، ومبدأ التفسير الضيق للنص

= www.ahu.edu.jo/tda/papers%5C89.doc

(1) د. عبد الفتاح بيومي حجازي، الحماية القانونية للتجارة الإلكترونية، مرجع سابق، ص 266.

الجنائي، ومبدأ القياس في تفسير النصوص الجنائية، مع مراعاة الأصول الثابتة للقواعد القانونية الجنائية، ويأتي في مقدمة هذه القوانين، قانون دوقية لكسمبرج في غرب أوروبا، حيث أتى بمفاهيم جديدة في قانون العقوبات المعلوماتي، تختلف عن تلك المقررة في قانون العقوبات التقليدي.

ولا شك أن هذه القوانين المعلوماتية تساهم إيجابًا في تنمية التجارة الإلكترونية وحمايتها، وتزرع الثقة لدى جمهور المتعاملين فيها، سواء أكانوا منتجين أم مستهلكين، وسواء أكانوا بائعين أم مشترين عبر الشبكة، وذلك لأن التجارة عبر الشبكة أصبحت رافدًا مهمًا للاقتصاد العالمي الجديد، والذي أضحى قرية كونية صغيرة بفضل ثورة الاتصالات التي يشهدها العالم، في حين أن التشريعات العربية بصفة عامة - ومنها التشريع المصري - مازالت بعيدة عن احتواء ظاهرة الجريمة المعلوماتية، وهو ما يؤثر سلبًا في تنمية التجارة الإلكترونية العربية[1]، حيث إنه وحتى الآن لم يصدر في الدول العربية سوى بضعة قوانين تهتم بالتجارة الإلكترونية، هي القانون التونسي الصادر عام 2000، والقانون الصادر في إمارة دبي برقم 2 لسنة 2002 في شأن التجارة والمعاملات الإلكترونية، والقانون الاتحادي الإماراتي رقم 1 لسنة 2006 بشأن المعاملات والتجارة الإلكترونية[2]، والقانون الاتحادي رقم 2 لسنة 2006 في شأن مكافحة جرائم تقنية أنظمة المعلومات، ونظام مكافحة جرائم تقنية المعلومات في المملكة العربية السعودية، وقانون المعاملات الإلكترونية البحريني، وقانون المعاملات

(1) د. عبد الفتاح بيومي حجازي، نظام التجارة الإلكترونية وحمايتها القانونية، مرجع سابق، ص 267.
(2) د. عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، دار الفكر الجامعي، الإسكندرية، ط ثانية، 2003، ص250.

الإلكترونية العماني، فضلا عن القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات.

بالإضافة إلى وجود عدد من مشروعات القوانين كمشروع القانون المصري في شأن التجارة الإلكترونية، وإن كان المشرع قد استجاب للمطالبات المتعددة بسرعة إصداره، وأصدر جزءًا مستقلا منه هو قانون التوقيع الإلكتروني رقم 15 لسنة 2004 والذي بدأ العمل به فعلا[1]، ومشروع التجارة الإلكترونية الكويتي، والفلسطيني، ومشروع القانون العربي للمعاملات والتجارة الإلكترونية، ومشروع قانون مكافحة جرائم تقنية المعلومات لدول الخليج العربية.

والحقيقة أن المشكلة ليست في صدور أو عدم صدور قوانين التجارة الإلكترونية حتى الآن، إنما المشكلة تنحصر في ضرورة تنقية القوانين القائمة أو إصدار قوانين جديدة لمعالجة ظاهرة الإجرام المعلوماتي، مع مراعاة الطبيعة الخاصة والمتميزة للجريمة المعلوماتية، ومنها جرائم الأموال التي قد تتعرض لها التجارة الإلكترونية[2].

ويضع الفقه الجنائي ضرورة أن تشمل التعديلات التشريعية المقترحة تجريم الأفعال ذاتها التي سبق للمشرع الفرنسي وأن جرمها بالقانون رقم 19 لسنة 1988، وهي تتعلق بتجريم التعدي على الأموال المادية والمعنوية في نطاق المعلوماتية، وسواء تعلقت بالحاسب الآلي وملحقاته، أو البرامج والبيانات الخاصة بها، وضرورة تجريم السرقة المعلوماتية للبرامج والمعطيات، وضرورة تجريم حالات الاستخدام غير المشروع للحاسب

(1) د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية 2005، ط أولى، ص 105.

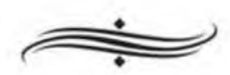
(2) د. عبد الفتاح بيومي حجازي، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 222.

الآلي، والمساواة في الحماية بين المال المادي والمعنوي، وتبني مفاهيم أكثر تطورًا في صياغة النصوص الجنائية تتفق مع ثورة المعلومات، لذلك يجب على السياسة الجنائية المتعلقة بحماية الأموال المعلوماتية أن تتبنى تفسيراً متطورًا للنصوص الجنائية.[1]

والخلاصة أن القواعد التقليدية في قانون العقوبات أضحت غير ملائمة لمواجهة جرائم السرقة والنصب وخيانة الأمانة والإتلاف في صورتها المعلوماتية حين تنصب على مال معنوي.

لذلك كان صدور القانون العربي الموحد في شأن مكافحة جرائم تقنية المعلومات خطوة نحو الطريق الصحيح، يجب أن يتبعها خطوة أخرى، وهي أن تتبنى التشريعات الوطنية هذا القانون وتزيد عليه أو تعدل فيه حسب ظروفها الداخلية.

وباكتمال مظلة التشريعات العقابية الخاصة بالجريمة المعلوماتية تكتمل حماية التجارة الإلكترونية، وتزداد الثقة فيها والإقبال عليها، بما يؤدي إلى نموها وتطورها مثل البلدان المتقدمة معلوماتيا.



(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 19, ود. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات، مرجع سابق، ص 36 وما بعدها.

المبحث الثالث

جريمة التزوير المعلوماتي

يعرف التزوير بأنه تغيير الحقيقة في محرر رسمي أو عرفي أو معلوماتي بإحدى الطرق التي حددها القانون، تغييراً يرتب ضرراً للغير عند استعماله فيما زور له[1].

وترجع علة العقاب في التزوير إلى رغبة المشرع في ضرورة كفالة الثقة في المحررات بوصفها وسيلة لا غنى عنها لإثبات الحقوق والمراكز القانونية، لتصير في نظر الناس معبرة عن الحقيقة، فيقدموا على التعامل بها بثقة واطمئنان، ولكي يؤدي المحرر دوره في منع كل نزاع في المستقبل بشأن محتواه وتكون البيانات التي يتضمنها المحرر عنوانًا للحقيقة، وإلا فقدوا ثقتهم فيه وأحجموا عن الاعتماد عليه في معاملاتهم، وهو ما يؤدي إلى اضطراب المعاملات وكثرة المنازعات.[2]

ويصور الفقه جريمة التزوير بأنها تغيير للحقيقة مقترن بقصد الغش، يقع في محرر بإحدى الطرق التي يبينها القانون، مسببًا ضررًا للغير، وعلى ذلك تقوم الجريمة موضوع البحث على ركنين أحدهما الركن المادي، والثاني الركن المعنوي، ونتناول في دراستنا للتزوير طرق التزوير المادية وطرق التزوير المعنوية، لنرى مدى انطباق كل منهما على جريمة التزوير المعلوماتي كل في مطلب على حدة.

المطلب الأول: طرق التزوير المادية في جريمة التزوير المعلوماتي

المطلب الثاني: التزوير المعنوي المعلوماتي

---

(1) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1988، ص 244.

(2) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، 1972، ص 279.

المطلب الأول

طرق التزوير المادية في جريمة التزوير المعلوماتي

يقوم الركن المادي في جريمة التزوير على نشاط يباشره الجاني ويتمثل في تغيير الحقيقة في محرر، باستخدام إحدى الطرق التي نص عليها القانون، ويكون من شأن تغيير الحقيقة أن يسبب ضررًا للغير، هذا بالنسبة للجريمة التقليدية المنصوص عليها في قانون العقوبات، والتساؤل هنا: إلى أي مدى يمكن وقوع جريمة التزوير في نطاق المعلوماتية؟ وبمعنى آخر: هل يتصور وقوع جريمة التزوير في صورتها العادية عن طريق استخدام الحاسب الآلي، أو بالدخول إلى شبكة المعلومات الدولية الإنترنت؟

سوف نجيب على هذا التساؤل بشرح طرق التزوير المادية في خمسة فروع: الأول: وضع إمضاءات أو أختام أو بصمات مزورة، والثاني: تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات، الثالث: وضع أسماء أو صور أشخاص آخرين مزورة، الرابع: التقليد، الخامس: الاصطناع، وذلك على النحو التالي:

الفرع الأول

وضع إمضاءات أو أختام أو بصمات مزورة

تعني هذه الطريقة من طرق التزوير المادية أن ينسب المزور محررًا إلى شخص لم يصدر عنه، حيث إن ظهور إمضاء شخص أو ختمه أو بصمته في محرر يعني أن ما يتضمنه المحرر قد صدر عنه، إذ الإمضاء وما في حكمه هو رمز الشخصية ودليلها.[1]

---

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص230.

ويكون الإمضاء مزورًا متى وضع الجاني إمضاء شخص آخر في المحرر، أو بتعبير آخر: " يضع إمضاءً ليس له في المحرر"، ويكتفي المشرع في ذلك بوضع الإمضاء ولا يتطلب تقليده.[1]

ويترتب على اعتبار الإمضاء مزورًا أن وضع الإمضاء في المحرر لم يكن تعبيرًا عن إرادة صحيحة لمن ينسب إليه المحرر، ومع ذلك ينسب إليه المحرر، ومثال ذلك أن يوقع شخص على محرر باسمه العائلي دون الاسم الشخصي بهدف أن ينسب المحرر إلى الاسم العائلي وليس إليه.[2]

أما الختم المزور فيكفي وضع ختم لشخص على المحرر، وهدفه نسبة المحرر لصاحب الختم مع أن إرادة ذلك الشخص لم تنصرف إلى ذلك، سواء قلد ختمًا لذلك الشخص واستعمله، أو تحصل على ختمه الحقيقي ووقع المحرر به، فالتزوير قائم حتى ولو كان الختم صحيحًا.[3]

وأما البصمة المزورة فهي تأخذ حكم الإمضاء، إذ نصت المادة (225) من قانون العقوبات المصري على أن: " تعتبر بصمة الأصبع كالإمضاء في تطبيق أحكام هذا الباب "، ويقصد بذلك الباب السادس عشر المتعلق بالتزوير، ومضمون ذلك أن البصمة هي بديل الإمضاء لشخص لا يستطيع التوقيع، وهي دليل على شخصية صاحبها.[4]

---

(1) نقض جنائي، جلسة 1936/1/6 مجموعة القواعد القانونية، ج4، رقم 29، ص 29، نقض جنائي، جلسة 1937/3/1 مجموعة القواعد القانونية، ج 4، رقم 52، ص 51، نقض جنائي، جلسة 1975/4/11 مجموعة أحكام النقض، س 6، رقم 50، ص 809.

(2) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 231.

(3) نقض جنائي، 1955/1/1، مجموعة أحكام النقض، س 6، رقم 445، ص 579.

(4) وضع هذا النص عام 1937 لحسم الخلاف بين أحكام القضاء، حيث اتجهت =

أما عن إمكانية وقوع التزوير المعلوماتي بهذه الطريقة فهو أمر وارد إذا ما تأملنا طبيعة ووظيفة جهاز الحاسب الآلي وشبكة المعلومات التي ترتبط بها هذه الحواسيب، سواء أكانت نظم معلومات داخلية أو شبكة المعلومات العالمية الإنترنت.

فمن المعلوم أن جهاز الحاسب الآلي - أيًا كان موقعه وأيًا كانت الجهة التي يخدم فيها - يتلقى بيانات يغذي عليها نظامه المعلوماتي وهي المدخلات، وهذه المدخلات تعكس العمليات والأنشطة التي تجري داخل الجهة سواء أكانت مؤسسة صناعية أم شركة تجارية أم وزارة، وهذه البيانات والمعلومات تتعلق بطبيعة نشاط الجهة كعدد العملاء المتعاملين معها وأصناف البضاعة وأسعارها، أو نشاط الوزارة، والخطط التي تنفذها... إلخ، وهذه المدخلات يقابلها ما يسمى بالمخرجات، وهي المعلومات الناتجة عن النظام المعلوماتي للحاسب الآلي، وهي أمور تحتاجها الجهة كي تصدر قرارها في الوقت المناسب، وما بين عملية (الإدخال والإخراج) يقوم الحاسب الآلي بعملية تحليل البيانات ومعالجتها للوصول إلى المخرجات التي تحتاجها الجهة[1]، إذ إن نظام الحاسب الآلي يعتمد على المعلومة، سواء أكانت هذه المعلومات محفوظة في داخله أو كان

= محكمة النقض إلى نفي المساواة بين الإمضاء والبصمة إذ سبق لها أن قضت بأنه: " أما البصمة التي يضعها شخص ما بإصبعه مستحيل عقلا أن تكون مزورة لا في ذاتها ولا في نسبتها لغير باصمها؛ لأنها لو نطقت لما فاهت إلا باسم المراد نسبتها إليه ".
نقض 251 في 1929/5/9، مشار إليه لدى د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 233.

(1) عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات - دراسة مقارنة - دار النهضة العربية، القاهرة 2000، ص 39 وما بعدها.

مصدرها شبكة معلومات أو نظام معلوماتي داخل الجهة نفسها مرتبط بجهاز رئيسي يمدها بما تحتاجه يسمى (الخادم)، أو تكون المعلومات مصدرها شبكة المعلومات الدولية (الإنترنت).

وطالما أن المتداول في جهاز الحاسب الآلي عبارة عن معلومة، وهذه المعلومات ذات قيمة في ترتيب حق أو أثر قانوني معين، فمن السهل تزوير مخرجات الحاسب المتضمنة هذه المعلومات.[1]

فهذه المخرجات قد تتمثل في قرار إداري من جهة حكومية يرتب أثرًا قانونيًا معينًا، ويكون ذلك القرار مرهونًا بتوقيع الوزير أو الرئيس الإداري الأعلى في الجهة مصدرة القرار، ومن السهل إدخال صورة توقيع الشخص المنسوب إليه التزوير عن طريق جهاز الماسح الضوئي المرتبط بالحاسب الآلي، ويضاف التوقيع للورقة التي انطوت على البيان المزور، وبذلك تكون قد اكتسبت صفتها الرسمية بعد أن دون فيها بيانات على غير إرادة صاحبها أو نسبت إليه دون أن تنصرف إرادته إلى ذلك.

وما يصدق على التوقيع يصدق كذلك على نموذج البصمة، وكذلك الختم الشخصي إذ يمكن وضعهما على نموذج لهما وإدخالهما على المستند المدعى نسبته لصاحب البصمة والختم على غير إرادة صاحبها وذلك عن ذات الطريق، وبذلك يمكن الحصول على مستند صحيح من الناحية الشكلية لكنه مزور بالنظر إلى أنه نسب إلى شخص بعد أن حمل إمضاءه أو بصمته أو ختمه على غير إرادته.

ومن الناحية العلمية أصبح ممكنًا أن ينقل لجهاز الحاسب الصور الشخصية أو غيرها، والتوقيعات والنصوص المطلوب ظهورها على شاشته

(1) Catala pierre Ebouche d'une bheonrie duriique de l'information D.S. 1974 P.97.

أو احتفاظه بها مع عدم استخدام طريقة الكتابة، وذلك باستعمال جهاز الماسح الضوئي، أو تلقي المعلومات عن طريق شبكة الإنترنت وإعادة معالجتها على نحو ما يريده المزور لتكون مخرجات الحاسب الآلي المزورة حسبما أراد الجاني.

والأصل في ذلك أن ما يتداول في الحاسب الآلي هو معلومة، وهذه المعلومة ذات قيمة اقتصادية وثقافية، وطالما أصبحت المعلومة ذات قيمة، فمن الممكن سرقتها[1] وبالتالي يمكن تزويرها.[2]

ولقد شهد التطبيق العملي لنشاط الحاسب حالات تزوير تضمنت إبرام صفقات وهمية بأسماء أشخاص وهمية[3]، أو الحجز لأماكن وهمية، أو

(1) Leclerq (Pierre) et Catala (Pierre)،L'information est, elle un bién informatique، Masson، 1992،p.91.

ويرى أن ظهور القيمة الاقتصادية للمعلومات أدى إلى ظهور قيمة لم تكن مألوفة من قبل، وأموال جديدة عرفت بالأموال المعلوماتية، وفي ذلك تصلح أن تكون محلا للسرقة كغيرها من الأموال، والمستندات المثبتة لها تصلح أن تكون محلا للتزوير على ما نرى.

(2) د. هلالي عبد اللـه، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص 29 وما بعدها.

(3) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 35.

- وبعد انتشار التعاقد بطريق شبكة الإنترنت، أدى ذلك إلى ظهور فئة من لصوص التجارة الإلكترونية يمكنها انتهاك بيانات الأفراد والمؤسسات المتصلة بشبكة الإنترنت، وذلك بالسطو عليها أو التلاعب فيها أو تحريفها، الأمر الذي يؤدي لخسائر جسيمة لهذه المؤسسات، الأمر الذي يتطلب ضمانات أمنية للبيانات المنقولة عبر شبكة الإنترنت منعًا للتزوير المعلوماتي، وذلك بإبرام صفقات وهمية بأسماء أشخاص آخرين.

طلب شراء سلع أو خدمات بأسماء أشخاص مزورة.[1]

ويرى بعض الفقه إمكانية وقوع التزوير المعلوماتي بوضع إمضاء مزور على المستندات المعالجة آليًا عن طريق الاستخدام غير المشروع للرقم الشخصي السري للدخول أو تقليد مستند معالج على ورقة.[2]

الفرع الثاني

تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات

ويقصد بهذه الطريقة كل ما يمكن إدخاله من تغيير مادي لصلب المحرر أو الإمضاء أو الختم الموضوع عليه، وذلك لإحداث تعديل في معناه، ويدخل ضمن هذه الطريقة الزيادة على كلمات المحرَّر.[3]

وقد كان المشرع - كما لاحظ جانب من الفقه - في غنى عن إيراد عبارة (أو زيادة كلمات)، وذلك لأن لفظ تغيير المحررات يشملها، ويقصد

(1) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 39.

- ويعد من صور التزوير المعلوماتي الحجز الوهمي لأماكن في وسائل النقل والفنادق، أو بطلب شراء سلع أو خدمات من خلال شبكة الإنترنت.
- وتقدم الشبكة خدمة Escrow house، وهى عبارة عن مؤسسة مالية ترسل لها النقود، كثمن للمنتجات المطلوبة من أي موقع بالشبكة، وتحفظ الأموال طرفها حتى يخطرها المشتري بأنه تسلم المنتجات طبقًا للمواصفات، وفي هذه الحالة يحول السعر للبائع، ويمكن للمشتري استرداد ما دفعه في حال ما إن ثبت أن المنتج غير مطابق للمواصفات أو لم يصله أصلا، ومواقع هذه المؤسسات على شبكة الإنترنت.

At: http:// www.iascrow.com

http://www.trade.direct.com

(2) د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 1997، ص 64.

(3) د. السعيد مصطفى السعيد، قانون العقوبات، القسم العام،، دار المعارف, القاهرة، ص 100.

بالتغيير هنا ذلك الذي يحدث بعد اكتمال المحرر والتوقيع عليه، أما التغيير الذي يحدث أثناء تحرير الورقة أو المحرر فهو تزوير معنوي.[1]

وتغيير المحررات قد يكون إما بالإضافة أو الحذف أو التعديل، وتحدث الإضافة بزيادة كلمة أو أكثر إلى اسم ورد في المحرر أو إلى الإمضاء أو بزيادة رقم لمبلغ مكتوب في محرر أو في التاريخ أو بزيادة كلمات في مكان خال من المحرر.[2]

وأما التغيير بالحذف فيكون بحذف كلمة أو رقم أو اسم أو عبارة وردت في المحرر، أيًا كانت الوسيلة التي استعملها المزور، سواء أكانت بالكشط أو الشطب أو المحو بمادة كيميائية أو جزء من المحرر بالحبر وخلافه، على أنه يلاحظ أن إعدام المحرر كله بإتلافه أو تمزيقه يخرج من نطاق التزوير ويندرج في عداد المادة (365) عقوبات مصري، والمادة (424) عقوبات إماراتي، المتعلقة بالعقاب على إتلاف المستندات.[3]

وأما التغيير بطريقة التعديل، فهو كما تعرفه أحكام النقض خليط ما بين

---

(1) د. عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1986، ص149.

(2) المرجع السابق، ص 155.

- وتشير إلى المعنى ذاته أحكام النقض: نقض جنائي، 1933/6/9، مجموعة القواعد القانونية، ج3، رقم 144، ص 169، نقض جنائي، 1950/11/28، مجموعة أحكام النقض، س 2، رقم 102، ص 273.

(3) نصت المادة (365) عقوبات مصري على أن: " كل من أحرق أو أتلف عمدًا بأي طريقة كانت شيئًا من الدفاتر أو المضابط الأصلية أو السجلات أو نحوها من أوراق المصالح الأميرية، أو الكمبيالات أو الأوراق التجارية أو المصرفية، أو غير ذلك من السندات التي يتسبب عن إتلافها ضرر للغير، يعاقب بالحبس، وبغرامة لا تتجاوز خمسمائة جنيه، أو بإحدى هاتين العقوبتين.

كل ذلك يؤكد تصور وقوع التزوير المعلوماتي للصورة عن طريق جهاز الحاسب الآلي والأجهزة المساعدة له، وذلك عن طريق رسم الصورة ضوئيًا ونقلها إلى جهاز الحاسب الآلي[1]، واستخراجها ورقيًا عن طريق طباعة الحاسب الآلي، أو إدخالها على بيانات مخزنة في ذاكرة الحاسب الآلي نفسه وعرضها على الشاشة دون طباعة ورقية، لاسيما وأننا نستطيع القول بأن التزوير المعلوماتي لا يتطلب المستند الورقي المكتوب أو المطبوع، وذلك لأن مخرجات الحاسب الآلي والتي يظهر فيها التزوير المعلوماتي قد تكون لا ورقية.[2]

الفرع الرابع

التقليد

ويقصد به المحاكاة، وهو في مفهوم التزوير إنشاء محرر على مثال محرر آخر[3]، أو أن يحرر المتهم كتابًا بخط يشبه خط شخص آخر، سعيًا

= وكذلك ما تضمنته إحدى القضايا التي تم تداولها بمحاكم أبو ظبي بدولة الإمارات العربية حينما قام أحد المشتركين بشبكة الإنترنت عن طريق استخدامه الماسح الضوئي ببث صور مخلة بالحياء العام، وإرسالها إلى المشتركين الذين تبدأ أسماؤهم بحروف (X y) من خلال البريد الإلكتروني الخاص بهم، وقد جرت محاكمته طبقًا لأحكام المادة 46 / 2 من قانون مؤسسة الإمارات للاتصالات, والمادة 362 من قانون العقوبات الاتحادي.

(1) د جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 43.

(2) وليد عالكوم، مفهوم ظاهرة الإجرام المعلوماتي، بحث مقدم في مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية، 2000، ص 5.

(3) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مؤتمر القانون والكمبيوتر والإنترنت، مرجع سابق، ص 15.

لأن ينسب إليه هذا المحرر[1]، والتعريف الأول أدق وأشمل لأنه ينصرف إلى إنشاء محرر مشابه لمحرر آخر، حتى لو لم يتضمن ذلك الاستعانة بالكتابة، بعيدًا عن المفهوم الضيق لنص المحرر أو البيانات المدونة فيه في نطاق التزوير، والتي كانت سببًا لأن يتدخل المشرع المصري وينص على تجريم التزوير عن طريق وضع صور أشخاص آخرين مزورة في المادة 211/عقوبات - مصري، كما أن هذا التعريف هو الذي يتفق مع إمكانية وقوع التزوير المادي بهذه الطريقة معلوماتيًا، ويستوي أن يكون المحرر مدونًا كتابة أو يحتوي على رموز وصور دون كتابة طالما أن لها دلالة معينة، كما في الرسومات الهندسية أو صور الحيوانات - حسب قانون دولة الإمارات في المادة (216) التي جرمت تزوير مطلق الصور أو صور الأشخاص كما في القانون المصري، إذ أصبح من الجائز جدًا عن طريق الحاسب الآلي وجهاز الإدخال والطابعة استخراج محرر طبق الأصل لمحرر موجود، وهذا هو التزوير بطريقة التقليد، حيث يكون من السهل وقوعه بطريقة التزوير المعلوماتي، ولا يشترط في التقليد أن يبلغ حدًا من الإتقان، بل تكفي المحاكاة على نحو ينخدع بها بعض الناس إلى حد وهمهم بصحة المحرر المقلد[2].

وتقوم جريمة التزوير بالتقليد في المحررات العرفية كالدفاتر التجارية والأوراق الخاصة التي تصلح كمبدأ ثبوت بالكتابة، أو في المحررات

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 238.

(2) نقض جنائي جلسة 1972/6/19، مجموعة أحكام النقض، ص 23، رقم 210، ص 940، وكذلك نقض جنائي، جلسة 1979/4/29، مجموعة أحكام النقض، س 30، رقم 2107، ص 506.

الرسمية كتذاكر السكك الحديدية.

ولا تقع طريقة التزوير هذه وحدها، وإنما غالبًا ترتبط بطريقة أخرى، فلو قام الجاني بوضع إمضاء أو ختم مقلد على المحرر المقلد، فقد توافر إلى جانب طريقة التقليد التزوير المادي وهو الذي يتمثل في تغيير المحررات أو الأختام أو الإمضاءات أو زيادة كلمات، كذلك قد يقلد الجاني خط الغير وينشئ محررًا جديدًا ينسب صدوره له، ففي هذه الحالة يتحقق التقليد وكذلك الاصطناع كمن يقلد تذاكر السكة الحديد أو أوراق اليانصيب[1].

ومع ذلك فإن طريقة التزوير بالتقليد قد تقع وحدها دون وقوع التزوير المادي، كتقليد خط الغير في محرر موقع على بياض، ففي هذا الفرض لا يضع الجاني إمضاءً مزورًا، ولا يغير المحرر أو اسمًا مزورًا، كما لا يصطنع المحرر، لأن الاصطناع يتطلب عمل محرر جديد، ولكن في المثال المذكور، فإن المحرر موقع من صاحب الشأن[2]، وهذه الطريقة يمكن أن تتم معلوماتيًا، وقد تحقق ذلك بالفعل بدولة الإمارات العربية المتحدة[3] حينما

(1) راجع في ذلك د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 264.

(2) من الفقه الذي يرى ذلك: د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 239، د. السعيد مصطفى السعيد، قانون العقوبات، القسم الخاص، مرجع سابق، ص 104، والفرض في هذه الحالة أن الجاني استولى على الورقة الموقعة على بياض خلسة من صاحبها، أما لو كانت سلمت له اختياريا فهو خائن للأمانة حسب المادة 340 عقوبات مصري، والمادة (404) عقوبات إماراتي، انظر في هذا المعنى: نقض جنائي، جلسة 1976/1/25، مجموعة أحكام النقض، ص 27، رقم 22، ص 100.

(3) القضية رقم 99/112 جنايات أمن دولة أبو ظبي، وتتلخص وقائع الدعوى في =

تم ضبط متهم بجريمة تزييف عملة نقدية باستخدام الحاسب الآلي في ارتكاب هذه الجريمة، وتمت محاكمته وفقًا لقانون العقوبات الإماراتي[1].

= قيام أحد الأشخاص وكان شابا في مقتبل عمره ويعمل كموظف حاسب آلي بإحدى الوزارات السيادية بالدولة، قام بتقليد الورقة النقدية من فئة (500) درهم إماراتي على نحو متقن ساعده في توزيعها بسهولة داخل مدينة العين وما حولها، وفي التحقيق مع المتهم المذكور بمعرفة النيابة العامة المختصة، قرر المتهم أن إقدامه على هذا الفعل كان نوعًا من تحدي الذات؛ إذ إنه يجيد التعامل مع الحاسب الآلي بمهارة وكذلك الملحقات المساعدة له، وهي الماسح الضوئي، والطابعة، وكان لديه ذلك الجهاز في منزله كحاسب شخصي له، وقد تم التحفظ عليه ضمن مضبوطات القضية، وقام بالحصول على نوعية من الأوراق شبيهة بتلك التي تستعمل في طبع ورق النقود، وأقلام رصاص لونها رصاصي لإدخال تعديلات أو ألوان معينة على الورقة المزورة بطريقة التقليد، وذلك لحل مشكلة الخط الأفقي الذي يتوسط هذه الورقة بوصفه من وسائل الأمان ضد تقليدها، وأضاف الجاني أنه قضى أيامًا عدة يحاول عن طريق حسابات هندسية معقدة حتى توصل إلى المقاسات المثلى بهذه الحسابات لكيفية خروج الورقة المقلدة، وكم كانت سعادته عظيمة عند رؤيته لها حيث بدأ في ترويجها، وقد قضي ضده بالسجن المؤقت لمدة خمس سنوات إعمالا للمواد 1/204، 205، 399... من قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة.

(1) تمت محاكمة المتهم وفقا لقانون العقوبات الإماراتي حيث:

- تنص المادة (204) من القانون ذاته على أن يعاقب بالسجن المؤبد أو المؤقت وبالغرامة كل من قلد أو زيف أو زور بأية كيفية كانت سواء بنفسه أو بواسطة غيره، عملة ورقية أو معدنية متداولة قانونًا في الدولة أو في أخرى، أو سندًا ماليًا حكوميًا، ويعتبر تزييفًا في العملة المعدنية إنقاص شيء من معدنها، أو طلاؤها بطلاء يجعلها شبيهة بعملة أخرى أكثر منها قيمة.
- كما تنص المادة (205) من القانون ذاته على أنه يعاقب بالعقوبة المذكورة في المادة السابقة كل من أدخل بنفسه أو بوساطة غيره في الدولة أو أخرج منها عملة أو سندًا مما ذكر في المادة السابقة، متى كانت العملة أو السند مقلدًا =

ووفقا لذلك فإننا نستطيع القول بإمكانية وقوع التزوير المعلوماتي بطريقة التقليد أيًا كان المحرر أو المستند الذي يتم تقليده، ولا يشترط أن يكون مكتوبًا، وإنما قد يتضمن صورة أو رموزًا معينة لها دلالة خاصة يجري تقليدها على نحو متقن.

الفرع الخامس

الاصطناع

تتمثل هذه الطريقة من طرق التزوير المادي في خلق محرر بأكمله ونسبته إلى غير محرره[1]، أو كما قالت محكمة النقض المصرية في هذا الشأن: إن الاصطناع هو إنشاء محرر بكامل أجزائه على غرار أصل موجود، أو خلق محرر على غير مثال سابق.[2]

وهناك فارق بين التقليد والاصطناع، ففي الاصطناع لا يهم الجاني مدى التشابه بين خطه وخط الغير عكس التقليد، وذلك لأنه يصنع محررًا جديدًا بكامله، بينما التقليد يعالج جزءًا من المحرر، وغالبًا يوقع على المحرر المصطنع بتوقيع مقلد، كي يستمد قيمته القانونية من هذا التزوير، ولكن

= أو مزورًا، وكذلك من روج شيئًا من ذلك أو تعامل به أو حازه بقصد الترويج أو التعامل، وهو في كل ذلك على علم بالتقليد أو التزييف أو التزوير.

- ويلاحظ أن قرار الإحالة في هذه القضية لم يوجه للمتهمين بالمادة (216) عقوبات التي حددت طرق التزوير ومنها التقليد، وذلك لأن المادة (1/204) من القانون ذاته خاصة بتزييف وتزوير العملة.

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 239.

(2) نقض جنائي، جلسة 1968/5/6 مجموعة أحكام النقض، ص 19، رقم 105، ص 536, وكذلك نقض جنائي، جلسة 1971/12/27، أحكام، س 22، رقم 200، ص 833.

ليس هناك تلازم بين الطريقتين فكلاهما طريقة مستقلة للتزوير[1].

والاصطناع باعتباره طريقة من طرق التزوير المادي هو إنشاء محرر بكامل أجزائه على غرار أصل موجود، أو خلق محرر على غير مثال سابق، ما دام المحرر في أي من الحالتين متضمنًا لواقعة تترتب عليها آثار قانونية، وصالحًا لأن يحتج به في إثباتها[2].

ومثال التزوير بالاصطناع في محرر رسمي من يصنع صورة حكم وينسب صدوره إلى محكمة معينة[3]، بل يقوم التزوير بطريقة الاصطناع ولو كان التوقيع على المحرر أو ختم الجهة الحكومية سليمًا طالما أنه قد تم الحصول عليه بطريق غير مشروع.[4]

وكما يقع الاصطناع في محرر رسمي فإنه يقع في محرر عرفي، كمن ينسب صك مديونية إلى آخر، وذلك عن طريق اصطناع أو اختلاق هذا الصك كما لو كان شيكًا أو مخالصة لم تصدر عن المدير المنسوب صدورها إليه، ولكن في التزوير العرفي بطريقة الاصطناع لابد من تزوير إمضاء الغير حتى يحتج عليه به.[5]

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 239.
(2) حكم محكمة تمييز دبي، بتاريخ 9 / 6 / 2008 في الطعن رقم 2008 / 176 جزاء.
(3) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 265, وراجع حول ذلك: نقض جنائي، جلسة 1937/3/22، مجموعة القواعد القانونية، ج 4، رقم 63، ص 60.
(4) نقض جنائي، جلسة 1945/2/5، مجموعة القواعد القانونية، ج 6، رقم 498، ص462.
(5) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص265.

وعلى ذلك فإن التزوير بطريقة الاصطناع له صورتان إحداهما أن يخلق المتهم محررًا لم يكن موجودًا من قبل، أما الثانية فهي أن يخلق محررًا آخر وذلك بعد التعديل في شروطه أو بدون تعديل فيها.[1]

وقد يتم التزوير بطريقة الاصطناع حين يقوم الجاني بجمع قصاصات ورق كانت عبارة عن محرر تم تمزيقه، ذلك أن التمزيق إعدام للمستند وجمعه من جديد يعد إنشاءً له.[2]

والاصطناع كطريقة للتزوير، وإن وقع غالبًا مقترنًا بطريقة أخرى للتزوير المادي فإنه لا مانع من وقوعه استقلالا.[3]

ومن المقرر أن التزوير يكون بجعل واقعة مزورة في صورة واقعة صحيحة، ويشمل كل تقرير لواقعة على غير حقيقتها، ويشترط صراحة للعقاب أن يكون تغيير الحقيقة في بيان مما أعد المحرر لإثباته، والاصطناع كطريق من طرق التزوير المادي هو إنشاء محرر بكامل أجزائه، أو خلق محرر على غير الحقيقة ما دام المحرر متضمنًا لواقعة تترتب عليها آثار قانونية وصالحة لأن يحتج به في إثباتها.[4]

كما أنه بالنسبة للقصد الجنائي في جريمة التزوير فإنه يتحقق متى تعمد الجاني تغيير الحقيقة في المحرر مع انتواء استعماله في الغرض الذي من

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص24.
(2) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 266.
(3) د. السعيد مصطفى السعيد، قانون العقوبات، القسم الخاص، دار المعارف, القاهرة، ص 106.
(4) حكم محكمة تمييز دبي، بتاريخ 22 / 9 / 2008 في الطعن رقم 2008 / 315 جزاء.

أجله غيرت الحقيقة فيه، وليس أمرًا لازمًا التحدث صراحة واستقلالا في الحكم عن توافر هذا الركن، ما دام قد ثبت وقوع تزوير المحرر من الجاني فإنه يلزم عن ذلك أن يتوافر في حقه ركن العلم بالتزوير ونية استعماله.(1)

ويمكن وقوع التزوير بطريق الاصطناع من خلال الحاسب الآلي بما يمكن اعتباره تزويرًا معلوماتيًا، إذ يمكن للجاني أن يدخل ما يريد من معلومات أو بيانات إلى جهاز الحاسب الآلي، وينسب صدورها إلى شخص ما أو جهة ما، ثم يقوم باستخراجها من جهاز الحاسب الآلي بوصفها منسوبة إلى ذلك الشخص أو تلك الجهة، وذلك لأن الاصطناع هو خلق محرر بأكمله ونسبته إلى غيره، وليس هناك صعوبة في عملية إدخال عناصر المحرر المراد تزويره إلى جهاز الحاسب سواء أكان عن طريق الماسح الضوئي، أو عن طريق لوحة المفاتيح، بل وعن طريق استدعاء المعلومات من شبكة المعلومات الدولية، ثم صياغتها في هيئة المحرر المزور الذي يطلبه الجاني، وبعد ذلك يقوم بطبعه خارج الجهاز واستعماله إن رغب في ذلك وتوافر له الشكل أو المظهر الذي يمكن عن طريقه إدخاله على الغير، ولذلك فوقوع التزوير المعلوماتي بهذه الطريقة هو أمر ممكن في ظل التقدم العلمي لجهاز الحاسب الآلي وملحقاته.

(1) حكم محكمة تمييز دبي، بتاريخ 20 / 11 / 2006 في الطعن رقم 2006 / 291 جزاء.

المطلب الثاني

التزوير المعنوي المعلوماتي

ينصب التزوير المعنوي على مضمون المستند أو ملابساته وظروفه دون شكله ومادته، ويقع بطريقتين هما تغيير إقرار أولي الشأن، وجعل واقعة مزورة في صورة واقعة صحيحة، أو واقعة غير معترف بها في صورة واقعة معترف بها[1]، وكلا الطريقتين تتميز عن الأخرى[2].

والتزوير المعنوي يؤدي إلى تغيير في مضمون المحرر أو في ظروفه وملابساته لا في مادته أو شكله، ولذلك فهو غالبًا يقع عند إنشاء المحرر، ولا يترك أثرًا ظاهرًا ينم عنه ويمكن الإحساس به وإدراكه، مما يؤدي إلى صعوبة في إثباته على عكس التزوير المادي الذي يثبت من فحص المحرر نفسه، في حين يثبت التزوير المعنوي من أمور أخرى تتيسر أحيانًا، وتتعذر أحيانًا أخرى، وهو ما يجعل جانب من الفقه يرى أن التزوير المعلوماتي لا يقع بإحدى طرق التزوير المعنوي التي تتحقق عند التعبير عن الأفكار؛ لأن التزوير المعلوماتي يقع بطرق التزوير المادية، وهي طرق لا تتوافر في التزوير المعنوي، مثل وضع إمضاء مزور على المستندات المعالجة لا تكون إلا عن طريق الاستخدام غير المشروع [3]، وسوف نعرض لطرق التزوير المعنوي في هذا المطلب، ومدى إمكان وقوع التزوير المعلوماتي

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص241.
(2) نقض جنائي، جلسة 1944/4/10، مجموعة القواعد القانونية، ج 26 رقم 333، ص 455.
(3) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص241.

بإحدى طرق التزوير المعنوي، وذلك على فرعين، الأول: تغيير إقرار أولي الشأن، والثاني: جعل واقعة مزورة في صورة واقعة صحيحة.

الفرع الأول

تغيير إقرار أولي الشأن

تتحقق هذه الطريقة بقيام كاتب المحرر بتغيير البيانات التي طلب منه كتابتها عند تدوينها[1]، وفي هذه الطريقة فإن الجاني لا ينسب كل بيانات المحرر المزور لنفسه، بل ينسب بعضها للغير، ثم إنه يخالف ما أملاه عليه الغير ويدون بيانات مخالفة أو مشوهة فيغير مضمون المحرر[2]، ولذلك فهذه الطريقة لا تتيسر إلا عند إنشاء المحرر، فضلا عن صعوبتها في الإثبات، ولا يتيسر ذلك إلا بمقارنة ما كتبه الجاني مع ما كان يجب عليه أن يكتبه، وتكمن الصعوبة في إثبات ما كان يجب عليه أن يكتبه.

وتفترض هذه الطريقة توافر الثقة بين الجاني وبين الغير الذي يدلي ببيانات أمامه، كالمأذون الذي يطلب منه إثبات نوع الطلاق بأنه رجعي، فيثبت أنه بائن، ورغم أنه أهل للثقة فهو يخالف ذلك، وكذلك المدين الذي يطلب منه الدائن أن يثبت مقدار مديونيته في صك فيثبت أنه أوفى بكل أو بجزء مخالفًا الحقيقة، ولا تنفي الثقة القصد الجنائي من قِبل الجاني، حتى لو ثبت أن هناك إهمالا من ذوي الشأن في مراجعة بياناتهم وأقوالهم التي أدلوا بها.[3]

(1) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 63.
(2) د. رمسيس بهنام، الجريمة والمجرم في الواقع الكوني، منشأة المعارف، الإسكندرية 1996، ص 186.
(3) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص108, وص 242.
=
= وفي المعنى ذاته: نقض جنائي، جلسة 1932/12/26، مجموعة القواعد القانونية ج 3، رقم 69، ص 102.

ويقع هذا التزوير المعنوي في محرر رسمي، كما قد يقع في محرر عرفي، ومن أمثلته في محرر رسمي تغيير الحقيقة في دفتر الأحوال عند إثبات شكوى عن جريمة معينة[1]، وإثبات المأذون لمهر أقل مما ذكره المتعاقدان[2].

وتفترض هذه الأمثلة أن الفاعل في تزوير المحرر الرسمي بالطريق المعنوي دائمًا موظف عام، وهو ما يقطع بإمكانية وقوع التزوير المعلوماتي بهذه الطريقة في ظل ما نشهده من توغل الحاسب الآلي في حياتنا العملية واليومية سواء في ذلك عمليات دفع الفواتير، وطلبات البيع والشراء، وجميع عمليات البنوك والشركات والمؤسسات أيًا كان حجمها[3]، فيتمثل التزوير المعنوي في قيام الموظف العام المختص بتغيير الحقيقة في البيان البنكي الذي يحصل على بياناته من ذوي الشأن، أو فاتورة التليفون بإثبات سداد جزء منها على حين أن صاحب الشأن سددها كاملة، أو يثبت التسوية المالية لمعاملات أحد العملاء قبل بنك من البنوك بالمخالفة للحقيقة، وكل ذلك يتم عند إنشاء المستندات المثبتة للمعاملات أو التي تبرئ ذمة ذوي الشأن، وذلك عن طريق الحاسب الآلي، ولهذا فالقائلون بعدم تصور وقوع التزوير المعلوماتي بالطرق المعنوية يخالفون الواقع نظرًا لاعتمادنا في الوقت

(1) نقض جنائي، جلسة 1941/12/8، مجموعة القواعد القانونية، ج 5، رقم 316، ص 593.
(2) نقض جنائي، جلسة 1946/12/16، مجموعة القواعد القانونية، ج 7 رقم 261، ص 258.
(3) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 61.

الحالي شبه الكامل على جهاز الحاسب الآلي وملحقاته في إنجاز المعاملات الحكومية وغيرها.

ومن أمثلة التزوير المعنوي في محرر عرفي أن يكلف المدين من قِبل الدائن بأن يؤشر على ظهر سند الدين بما يفيد سداده لجزء من الدين، فيؤشر بسداد الدين كله أو بمعظمه على خلاف الحقيقة[1]، كذلك فقد يكلف شخص بترجمة مستند من اللغة العربية أو العكس، فيقوم بذلك مع تغيير مضمون المستند الذي تمت الترجمة إليه[2]، فهذه كلها محررات عرفية تم تغيير الحقيقة بها بالطريق المعنوي، وذلك بتغيير إقرارات أولي الشأن.

ولا صعوبة في أن تتم طريقة التزوير هذه بالطريق المعلوماتي، ذلك أن حسابات المؤسسات والشركات في الوقت الحالي غالبًا ما تتم عن طريق الحاسب الآلي، عبر برامج حساسة مخزنة على هذه الحاسبات معلوماتيًا، كما أن أعمال الترجمة شهدت تقدمًا، فأمكن إدخال النص المطلوب ترجمته لجهاز الحاسب بأي مدخل، وبعد ذلك يفتح برنامج معين للترجمة يكون مستخدمًا في الجهاز، فيتحول النص العربي للغة التي يريدها الشخص أو العكس، وبعد تمام الترجمة يمكنه التغيير فيها كيفما شاء.[3]

وفي النهاية فإن تغيير إقرارات أولي الشأن باعتبارها الطريقة الأولى للتزوير المعنوي يمكن وقوعها بطريق التزوير المعلوماتي، وسواء كان

(1) نقض جنائي، 1936/5/18، مجموعة القواعد القانونية، ج 3 رقم 473، ص 603.
(2) د. رمسيس بهنام، الجريمة والمجرم في الواقع الكوني، مرجع سابق، ص 187.
(3) ومن أمثلة طرق الترجمة الفورية البرامج الخاصة بالترجمة كبرنامج الوافي وغيره, أو المواقع التي تقدم خدمة الترجمة على شبكة المعلومات الدولية شبكة الإنترنت كموقع جوجل www.google.com , وموقع عجيب www.ajeep.com، وعن طريقه يمكن ترجمة أي نص أو موقع باللغة الإنجليزية للعربية فورًا أو العكس.

ذلك في محرر رسمي حرره موظف عام أو في محرر عرفي فيما بين ذوي الشأن، بما يتوافق مع تزايد وانتشار الحاسب الآلي والمعلوماتية في كافة مناحي الحياة.

الفرع الثاني

جعل واقعة مزورة في صورة واقعة صحيحة

تتمثل هذه الطريقة في إثبات واقعة على غير حقيقتها[1] بمعرفة كاتب المحرر، وعلى ذلك فكل تشويه أو تحريف يدخله كاتب المحرر على الوقائع التي يثبتها فيه عند تدوينه للمحرر يعد تزويرًا معنويًا بهذه الطريقة.

وتعد هذه الطريقة للتزوير المعنوي هي الأكثر اتساعًا، إذ تسع تغيير إقرارات أولي الشأن، كما يدخل في نطاقها جعل واقعة غير معترف بها في صورة واقعة معترف بها، طالما أن هذه الطريقة للتزوير المعنوي تعني كل إثبات لواقعة في محرر يغاير حقيقتها.[2]

وهذه الطريقة للتزوير المعنوي تتم في المحررات الرسمية وكذلك المحررات العرفية، وإذا تمت في المحررات الرسمية فالفاعل الأصلي في الجريمة دائمًا موظف عام.[3]

ومن تطبيقات محكمة النقض المصرية في شأن التزوير المعنوي في المحررات الرسمية بهذه الطريقة ما قضت بتوافره عندما يثبت المحقق في محضر التحقيق أنه لم يعثر في مسكن المتهم على أشياء تفيد في إثبات

(1) نقض جنائي، 1967/6/12، مجموعة أحكام النقض، س 8، رقم 157، ص 87.
(2) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص244
(3) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص268.

الجريمة، في حين أنه عثر على هذه الأشياء بالفعل، أو أن يثبت المأذون خلو الزوجة من الموانع الشرعية في حين أن هذه الموانع متوافرة[1]، وكذلك ادعاء الجاني أنه وكيل عن المدعى عليه في دعوى مدنية وذلك بالمخالفة للحقيقة.[2]

والحقيقة أن التطبيقات القضائية المذكورة تعكس جرائم وقعت ولا تزال تقع حتى اليوم، ولكن الفارق بين الماضي والحاضر هو في أسلوب ونوع الجريمة أو كيفية ارتكابها، والواقع أن الحاسب الآلي أضحى الأوسع انتشارًا في المحاكم والوزارات والمدارس والجامعات والمواصلات وغيرها، ولذلك فمن المتصور أن يقوم موظف الميكروفيلم المطلوب منه تدوين الأحكام وتوثيقها بالتلاعب في مضمون الحكم على غير الحقيقة، وتعد النسخة المحفوظة غير مطابقة للحكم الصادر، أو يقوم الموظف المختص بتقدير الرسوم في الدعاوى المدنية بالتلاعب في مقدار الرسم المطلوب دفعه توصلا لتخفيف أو تشديد الرسم قِبل المدعي، وذلك بمقتضى القسيمة التي يستخرجها من الحاسب الآلي الذي يدون عليه هذه البيانات.

كذلك فإن هناك بعض أجهزة التحقيق كالنيابة العامة في إمارة دبي بدولة الإمارات العربية المتحدة فقد شرعت فيما يسمى بالتحقيق الإلكتروني أو التحقيق عن بُعد، ويعني اجتماع المحقق عضو النيابة العامة والمتهم في محبسه، وكذلك الشهود بما فيهم رجال الضبط في أماكنهم، وذلك عن طريق دوائر تلفزيونية مغلقة عن طريق جهاز الحاسب الآلي، ويدور التحقيق

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص243.
(2) نقض جنائي، جلسة 1967/6/12، مجموعة أحكام النقض، س 18، رقم 157، ص871.

وكأنهم جميعًا في حجرة واحدة وجها لوجه.

وهناك أخطاء قد تحدث في التحقيق الجنائي العادي تعد تزويرًا كإثبات واقعة لم يتم الإدلاء بها خاصة اعتراف المتهم، أو عدم إثبات واقعة معينة، أو الخطأ عن عمد في تدوين اسم المتهم، أو مكان حصول الواقعة أو زمنها، أو وقت تنفيذ الإجراء الجنائي على نحو يفيد المتهم أو يضره، وكل تلك الوقائع كما يحدث التزوير المعنوي فيها من خلال الأوراق يحدث التزوير فيها من خلال الحاسب الآلي، كالتزوير في التحقيق الإلكتروني، أو التحقيق الجنائي عن بعد الذي يعد نموذجًا مثاليًا لجعل واقعة مزورة في صورة واقعة صحيحة بالطريق المعلوماتي.[1]

وأما عن التزوير بهذه الطريقة في المحررات العرفية فيقوم مثلا متى أثبت محصل في شركة تجارية المبالغ التي حصلها من عملائه في دفتر القسائم بأقل من المبالغ التي قبضها منهم، ولذلك فهذه الطريقة للتزوير المعنوي في المحرر العرفي تقع كذلك بطريقة الحاسب الآلي لزيادة انتشاره في الوقت الحاضر، فقل أن تجد هيئة أو شركة إلا وتعتمد على الحاسب الآلي في كافة ما تقوم به من عمليات سواء تجارية أو إدارية، وتعد ما تصدره من قسائم من مخرجات الحاسب الآلي التي يمكن التلاعب في

(1) عقد مؤتمر عن الحكومة الإلكترونية، في المركز التجاري الدولي بدبي في الفترة 21، 22 /2001/1 . وتطرق إلى التحقيق الجنائي الإلكتروني ومشكلاته العملية، وجدير بالذكر أنه يسجل لحكومة إمارة دبي اهتمامها بالمعلوماتية والأخذ بأسبابها في كل المجالات بما فيها أجهزة التحقيق، ولكن يبقى التشريع فاصلا في تغطية كل هذه الأمور، وهو أمر مهم يجب عدم إغفاله، خاصة وأن التحقيق الجنائي الإلكتروني ما زال منظما بقرارات إدارية من النائب العام لإمارة دبي، راجع أعمال المؤتمر المذكور، مؤسسة (داتا ماتكس) للمؤتمرات بدبي يومي 21، 2003/1/22م.

مضمونها فضلا عن قراءة بياناتها قبل طبعها واستخراجها من طابعة جهاز الحاسب الآلي[1].

وأمثلة التزوير في محررات عرفية بهذه الطريقة كثيرة لا تعد ولا تحصى، وعمومًا فإنها تمثل في مجملها إثبات ما يخالف الحقيقة أو يغيرها.[2]

ولما كان الحاسب الآلي قد أضحى بمثابة الكاتب والدفتر والمحاسب فإن التزوير المعلوماتي بهذه الطريقة أصبح في حكم المؤكد، عدا التحقيق الجنائي، وذلك لأنه في التحقيق الجنائي توجد وسائل عديدة للتثبت من شخصية المتهم، فهناك البصمات العادية لأصابع اليد، وهناك البصمة الصوتية، وهناك الصورة الشخصية، وفصيلة الدم، والخلايا التي يمكن عن طريق فحصها التثبت من شخصية الإنسان، ثم هناك كذلك ما يسمى بالحامض النووي DNA وهو نوع من التحليل يمكن عن طريقه أن يثبت على وجه اليقين شخصية الإنسان.

ويعد التزوير المعنوي بانتحال شخصية الغير سواء أكان هذا الغير موجودًا بالفعل أم شخصية خيالية[3] يدخل ضمن هذه الطريقة، ومن أمثلتها من يدلي بشهادته في الجلسة باسم منتحل[4]، أو انتحال شخصية الغير أمام

(1) نقض جنائي، 1927/1/4، مجلة المحاماة، س 7، رقم 491، ص 865.

(2) نقض جنائي، 1941/1/20، مجموعة القواعد القانونية، ج 5، رقم 188، ص 356. نقض جنائي، 1942/10/26، مجموعة القواعد الجنائية، ج 5، رقم 445، ص 594.

(3) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص244.

(4) نقض جنائي، جلسة 1938/6/20، مجموعة القواعد القانونية، ج 4، رقم 244، ص272.

الطبيب الشرعي[1]، أو في محضر البوليس، أو في محضر تحقيق جنائي[2].

وهذه الصورة للتزوير تحدث غالبًا في المحررات الرسمية، بأن يثبت الموظف في محرره اسم شخص غير من حضر أمامه[3]، وقد يقترن بهذه الصورة التزوير المادي بالمعنوي كأن يقترن انتحال الشخصية بإمضاء مزور.[4]

ويلحق بطريقة جعل واقعة مزورة في صورة واقعة صحيحة التزوير بالترك، وهو وقوع التزوير بفعل سلبي، كأن يتعمد من عهد إليه بكتابة المحرر أن يغفل بيانًا فيه بشرط أن يكون البيان مهما فيؤدي تركه إلى تغيير مضمون المحرر عما كان متفقًا عليه.[5]

ومن أمثلته امتناع كاتب العقد عن ذكر شرط جزائي اتفق عليه الطرفان[6]، وامتناع المأذون عن ذكر شرط اشترطته الزوجة يجعل العصمة في يدها، وامتناع موظف البريد عن ذكر بعض المبالغ التي أودعها

---

(1) نقض جنائي، جلسة 1950/3/27، أحكام النقض، س 1، ص 57، رقم 315.
(2) نقض جنائي، جلسة 1948/11/3، مجموعة القواعد القانونية، ج 7، رقم 672، ص636.
(3) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 244.
(4) نقض جنائي، جلسة 1979/4/26، مجموعة القواعد القانونية، س 30، رقم 106، ص 502.
(5) د. رمسيس بهنام، الجريمة والمجرم في الواقع الكوني، مرجع سابق، ص 190
(6) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص245.

المدخرون في صندوق التوفير في يوم معين[1]، والبعض يرى صعوبة وقوع التزوير المعنوي بطريقة الترك[2] باعتباره نوعًا من السكوت لا يقع به الفعل المجرم.

ولكن الفقه استقر على وقوع التزوير المعنوي بالترك، كما استقر عليه القضاء، حيث قضي بأن: (الرأي القائل بأن التزوير بطريقة الترك لا عقاب عليه لأن الترك لا يعد تغييرًا للحقيقة، إذ التغيير يقتضي عملا إيجابيًا من جانب مرتكبه، والذي يترك شيئًا كان يجب إثباته لا يأتي عملا إيجابيًا - هذا الرأي على إطلاقه غير سديد، إذ يجب ألا يقصر النظر على الجزء الذي حصل تركه، بل ينظر إلى ما كان يجب أن يتضمنه المحرر في مجموعه، فإذا ترتب على الترك تغيير في مؤدى هذا المجموع اعتبر الترك تغييرًا للحقيقة، وبالتالي تزويرًا معاقبًا عليه).[3]

كما أن محكمة النقض قضت أيضًا بأن الترك يقع به التزوير، [4]والذي يعد من طرق التزوير المعنوي بشرط أن يترتب عليه تغيير في المضمون الكلي لمعنى المحرر عما كان يجب أن يكون عليه[5]، والتزوير بالترك

---

(1) د. عوض محمد، قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، 1991، ص 205.
(2) راجع في عرض هذه الآراء والرد عليها: د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 244.
(3) نقض جنائي، جلسة 1935/2/4، مجموعة القواعد القانونية، ج 3، رقم 328، ص417.
(4) نقض جنائي، جلسة 1943/5/31، مجموعة القواعد القانونية، ج 6، رقم 200، ص274.
(5) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص273.

يختلف عن التزوير بالفعل الإيجابي، في أنه يعاصر لحظة نشوء المحرر، أما التزوير الإيجابي فقد يعاصر نشوء المحرر وقد يتراخى إلى ما بعد ذلك، ولكن كلاهما يتفقان في أنهما يؤديان إلى تغيير الحقيقة في المحرر، وذلك هو مناط التجريم[1].

ومن المؤكد وقوع التزوير المعلوماتي بطريقة الترك، وذلك بسبب بسيط هو أن الحاسب الآلي أصبح عصب الحياة في وزارات الحكومة وشركات القطاع الخاص[2]، ومن الأمثلة على ذلك أن يمتنع أحدهم عند ذكر تاريخ ميلاد الموظف في البيانات الخاصة به تحايلا على استمراره في الخدمة رغم بلوغ سن الإحالة للمعاش، ويستمر في وظيفته رغم إحالته للمعاش.

والفقه يتفق على أن جعل واقعة غير معترف بها في صورة واقعة معترف بها صورة من صور التزوير المعنوي وليست صورة مستقلة، وإنما تدخل ضمن "جعل واقعة مزورة في صورة واقعة صحيحة" ومثالها أن يثبت مأمور الضبط واقعة اعتراف المتهم على حين أنه لم يعترف، أو يثبت الموثق أن البائع قد أقر بقبض الثمن على حين أنه لم يقر بذلك، فالثابت في هذين المثالين أن الواقعة المزورة، أي الواقعة المدعى حصولها وهي الاعتراف أو قبض الثمن هي واقعة مزورة، وغير معترف بها، وأن هذا التزوير جعلها واقعة معترفًا بها، على حين أن المتهم لم يعترف، كما أن البائع لم يقر بقبض الثمن.[3]

(1) د. عوض محمد، قانون العقوبات، القسم الخاص، مرجع سابق، ص 206.

(2) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، 2000،ص 5, ويرى أن هناك أمثلة كثيرة للدلالة على التزوير المعلوماتي في نطاق سرقة بطاقات الائتمان وتقليدها وتزويرها.

(3) د. رمسيس بهنام، الجريمة والمجرم في الواقع الكوني، مرجع سابق، ص 190.

وأهم تطبيقات هذه الصورة في التزوير المعنوي حالتا انتحال الشخصية والتزوير بالترك.[1]

وقد أتى التقدم العلمي بنماذج من الجريمة تعجز النصوص القائمة عن ملاحقتها، كذلك فإن المشرع عاجز عن ملاحقتها بذات السرعة التي يتطور بها السلوك الإجرامي لوجود صعوبات تتمثل في عدم اتفاق المشرعين في الدول المختلفة أو فقهاء القانون في الدولة الواحدة على مفاهيم محددة لنماذج الجريمة، وهذا أمر طبيعي لكون التطور من سمات الحياة والبشر، لكن ما ينبغي التنويه إليه هو أنه يجب على ذوي الشأن من مشرعين وقضاة وفقهاء قانون وضع القواعد الملائمة والمناسبة بالسرعة الكافية لأي ظاهرة جديدة يترتب عليها سلوك إجرامي، لأن ظاهرة الجريمة هي ظاهرة مرتبطة بالسلوك الإنساني في كل حين، حتى ولو لم تقنن هذه القواعد، فسوف تقنن في يوم ما.[2]

وبذلك العرض لطرق التزوير المادي والمعنوي، نكون قد عرضنا من خلالها للإجابة على التساؤل الأول وهو مدى إمكانية وقوع التزوير المعلوماتي بهذه الطريقة.

وأخيراً نجد أن الفقه في مصر والإمارات العربية يكاد يكون متفقًا على أن التزوير المعاقب عليه لابد وأن يتم بإحدى الطرق التي نص عليها

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 243.

(2) د. غنام محمد، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، مرجع سابق، ص 7.

وفي المعنى ذاته: د. عمر الفاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، جامعة الإمارات، 1-3 مايو 2000، ص 122.

القانون، ذلك أنه لا يكفي لعقاب المزور أن يغير الحقيقة بطريقة ما، ولكن يجب أن يكون ذلك بإحدى الطرق التي نص عليها القانون.[1]

ويستند الفقه في ذلك إلى أن المشرع حرص على حصر الدائرة التي يعتبر تغيير الحقيقة فيها تزويرًا معاقبًا عليه، وذلك حتى لا يوصم كل كذب مكتوب بأنه تزوير.[2]

ومحكمة النقض المصرية بدورها قضت بأن " القانون أورد على سبيل الحصر الطرق التي تقع بها جريمة التزوير، بحيث لا يجوز توقيع عقاب فيها على أي تغيير للحقيقة بغير هذه الطرق، وأنه يجب أن يذكر في الحكم الصادر بالإدانة في التزوير كيفية ارتكابه بأية طريقة من الطرق التي عينها القانون".[3]

كما أن المشرع حدد طرق التزوير على سبيل الحصر في المواد 206، 208،211، 212، 213، 215، 217، 221 من قانون العقوبات المصري، والتي تحدد طرق التزوير التي نص عليها المشرع، ويسري ذلك على التزوير المادي والتزوير المعنوي.[4]

أما قانون العقوبات الاتحادي في دولة الإمارات العربية المتحدة، فقد

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 227.

(2) عرف التزوير بأنه إظهار الكذب في محرر بمظهر الحقيقة، وذلك غشا لعقيدة الغير، ذلك أن المشرع لم يجرم كل الأكاذيب المكتوبة، وهذا التجريم هو الحد الفاصل بين الكذب الذي يعد تزويرًا أم لا، د.رمسيس بهنام، الجريمة والمجرم في الواقع الكوني، مرجع سابق، ص 161.

(3) نقض جنائي، جلسة 1939/12/18، مجموعة القواعد القانونية، ج 5، ص 48، رقم 31.

(4) د. السعيد مصطفى، قانون العقوبات، القسم العام، مرجع سابق، ص 94.

أوردت المادة (216) منه طرق التزوير المادي والمعنوي على السواء، ولا تقوم جريمة التزوير إلا إذا كان تغيير الحقيقة قد تم بإحداها, حيث نصت المادة على أن: (تزوير المحرر هو تغيير الحقيقة فيه بإحدى الطرق المبينة فيما بعد تغييرًا من شأنه إحداث ضرر وبنية استعماله كمحرر صحيح، ويعد من طرق التزوير:

1) إدخال تغيير على محرر موجود سواء بالإضافة أو الحذف، أو التغيير في كتابة المحرر أو الأرقام أو العلامات أو الصور الموجودة فيه.

2) وضع إمضاء أو ختم مزور، أو تغيير إمضاء أو ختم بصمة صحيحة.

3) الحصول بطريق المباغتة أو الغش على إمضاء أو ختم أو بصمة لشخص دون علم بمحتويات المحرر أو دون رضاء صحيح به.

4) اصطناع محرر أو تقليده ونسبته إلى الغير.

5) ملء ورقة ممضاة أو مختومة أو مبصومة على بياض بغير موافقة صاحب الإمضاء أو الختم أو البصمة.

6) انتحال الشخصية أو استبدالها في محرر أعد لإثباتها.

7) تحريف الحقيقة في محرر حال تحريره فيما أعد لإثباته).

وفي فرنسا، نصت المادة (441) من قانون العقوبات الجديد على تجريم التزوير في المحررات الرسمية أو العرفية، والذي يقع بأي طريقة، وأصبح ذلك النص بعموميته يغطي التزوير المعلوماتي والتزوير بالطرق التقليدية.[1]

---

(1) نصت الفقرة (1) من المادة (441) عقوبات فرنسي على أنه: " يعد تزويرًا كل تغيير وتدليس للحقيقة، يكون من شأنه أن يحدث ضررًا، بأي وسيلة كانت، سواء وقع في محرر أو سند أيا كان موضوعه، والذي أعد مسبقًا كأداة لإنشاء حق أو ترتيب أثر قانوني معين، ويعاقب على التزوير واستعمال المحرر المزور بالسجن=

= ثلاث سنوات والغرامة التي لا تتجاوز 45.000 يورو ".

ARTICLE 441،1

(Ordinance no. 2000.916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January2002)

Forgery consists of any fraudulent alteration of the truth liable to cause harm and made by any means in a document or other medium of expression of which the object is, or effect may be, to provide evidence of a right or of a situation carrying legal consequences.

Forgery and the use of forgeries is punished by three years' imprisonment and a fine of €45,000.

أما الفقرة الثانية من المادة (441) من قانون العقوبات الفرنسي فقد عاقبت بالسجن لمدة سبع سنوات وغرامة 75.000 يورو عندما يرتكب التزوير أو يستعمل التزوير:

1) إما بواسطة شخص مؤتمن على السلطة أو مكلف بخدمة عامة، ويكون قد تصرف في حدود وظائفه.
2) وإما بطريقة اعتبارية.
3) وإما بقصد تسهيل ارتكاب جريمة، أو بقصد مساعدة فاعل الجريمة على الإفلات من العقاب.

ARTICLE 441،2

(Ordinance no. 2000.916 of 19 September 2000 Article 3 Official Journal of 22 September 2000 in force 1 January2002)

Forgery committed in a document delivered by a public body for the purpose of establishing a right, an identity or a capacity, or to grant an authorization is punished by five years' imprisonment and a fine of €75,000.

The use of a forgery specified in the previous paragraph is subject to the same penalties.

The penalty is increased to seven years' imprisonment and to a fine of €100,000 where the forgery or the use of the forgery is committed:

1° by a person holding public authority or discharging a public service mission acting in the exercise of his office;

2° habitually;

3° or with the intent to facilitate the commission of a felony or to gain impunity for the perpetrator.

ويبدو أن عمومية النص على النحو الوارد به مقصودة من المشرع الفرنسي، خصوصًا بعد أن تشابكت العلاقات وتطورت الحياة الاقتصادية، وانتشر الحاسب الآلي، وهو ما دفع المشرع الفرنسي أن يضفي حجية على هذه المحررات باعتبارها وثائق معلوماتية حماية للثقة العامة فيها[1].

وقد أيد البعض في مصر ودولة الإمارات العربية موقف المشرع الفرنسي في أن طرق التزوير لم ترد في القانون على سبيل الحصر، ليتوافق ذلك مع طبيعة وفلسفة الجريمة المعلوماتية.

فجريمة التزوير المعلوماتي ظهرت على إثر انتشار الحاسب الآلي وشبكة المعلومات الدولية، بل إن فكرة المحرر في التزوير التقليدي ويقابله الوثيقة المعلوماتية في التزوير المعلوماتي لم يصل الفقه إلى تعريف محدد في شأنها، ولقد عالجها المشرع في بعض البلدان مثل فرنسا، ومع ذلك لم يتم الوصول إلى مفهوم محدد في شأن الوثيقة المعلوماتية التي يقع فيها التزوير المعلوماتي، لاسيما وأن هذه الوثيقة تتجاوز فكرة المحرر المكتوب الذي ينصب عليه التزوير[2]، ويتصور أن تكون هذه الوثيقة المعلوماتية المزورة ضمن المخرجات الورقية للحاسب الآلي أو اللاورقية مثل شرائط مسجلة أو أسطوانات مدمجة أو حتى نصوص تظهر على شاشة الحاسب الآلي.[3]

(1) G. Bertin et al.، De lambertaire، la proctection du logiciel، en feux juridiques، p.33.

(2) Ben Halima (sassi) "Les crimes informatiques et d'autre crimes dans le domaine de la tachnologie informatique en Tunisie"، R.I.D.، 612.

(3) د. هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، مرجع سابق، ص 22.

وحول مدى انطباق النصوص الجنائية التقليدية القائمة والخاصة بجريمة التزوير المعلوماتي، فقد انقسم الفقه إلى رأيين مؤيد ومعارض، ولكل منهم حجته في ذلك.

الرأي الأول ذهب فيه جانب من الفقه إلى عدم انطباق نصوص التزوير التقليدية في حالة التزوير المعلوماتي، وقرروا أنه لقيام جريمة التزوير يشترط أن نكون بصدد محرر يصلح محلا لجريمة التزوير، ويجب أن يتخذ هذا المحرر شكل الكتابة، وعلى ذلك فإن صور التعبير عن الفكر الإنساني التي لا تتخذ شكل الكتابة لا تعد من قبيل المحررات حتى ولو كانت من قبيل المستندات، لذلك فالمستندات الإلكترونية لا تعتبر من قبيل المحررات الورقية[1].

وأضاف أصحاب هذا الرأي أن التزوير حين يقع على المعلوماتية لا يعد تزويرا لأن التلاعب تم في معلومات وبيانات مخزنة في الحاسب الآلي، ولم تظهر بعد على دعامة مادية كورقة مطبوعة أو شريط ممغنط أو قرص مدمج، وبالتالي لا ينطبق عليه وصف المحرر.

وذهبوا إلى أن طرق التزوير واردة في القانون على سبيل الحصر وليس من بينها التزوير الواقع على المحررات أو المستندات الإلكترونية، وقرروا أنه لا يكفي لعقاب المزور أن يغير الحقيقة بطريقة ما، ولكن يجب أن يكون ذلك بإحدى الطرق التي نص عليها القانون، وأن المشرع من جراء ذلك حرص على حصر الدائرة التي يعتبر فيها تغيير الحقيقة تزويرًا معاقبًا عليه، وذلك حتى لا يصير كل كذب مكتوب تزويرًا.

أما الرأي الثاني فقد ذهب إليه جانب آخر من الفقه، ونادى بتطبيق النصوص الخاصة بجريمة التزوير القائمة في قانون العقوبات على التزوير

(1) د. السيد عتيق، جرائم الإنترنت، مرجع سابق، ص 122.

الإلكتروني وما يشمله من تزوير للمحررات والمستندات المعالجة إلكترونيًا وتزوير التوقيع الإلكتروني بصفة خاصة، وأطلقوا عليها عملية التزوير المعلوماتي، وقالوا بانطباق نصوص جريمة التزوير عليها، واستندوا إلى عدة أدلة في ذلك.

حيث قالوا بأن التزوير المعلوماتي هو تغيير الحقيقة في المستندات المعالجة آليًا والمستندات المعلوماتية، وذلك بنية استعمالها، وعرفه جانب آخر بأنه تغيير الحقيقة بأي وسيلة كانت، سواء كان ذلك في محرر أو دعامة أو سند، طالما أن هذه الدعامة ذات أثر في إنشاء حق أو لها شأن في إحداث نتائج معينة[1].

وذهب أصحاب هذا الرأي إلى المساواة بين المستند الورقي والمستند الإلكتروني، وقرروا أن سجلات الحاسب الآلي ومخرجاته وما يسجل في ذاكرته والأسطوانات والشرائط الممغنطة تعتبر من قبيل المستندات.

واعتبروا أن المستند هو كل أسلوب لتحديد فكر أو فكرة على ورقة مكتوبة أو من خلال صوت أو صورة مسجلة، وأن المستند الإلكتروني هو المفهوم الحديث للمحرر في جريمة التزوير، فالهدف من الكتابة هو فهم وإدراك المعنى الذي يحمله المحرر، والمستقر عليه فقهًا وقضاءً أن المحرر لا عبرة فيه بالأداة التي استخدمت في الكتابة، وكل ما يتطلبه القانون لكي يعتبر المكتوب محررًا أن يكون تقريرًا لواقعة أو تعبيرًا عن إرادة يرتب القانون عليها أثرًا، وبالتالي فإن المستند الإلكتروني ما دام يمكن قراءته وإدراك معناه فهو والمحرر سواء[2].

(1) د. عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 139.
(2) د. السيد عتيق، جرائم الإنترنت، مرجع سابق، ص 124.

والمشرع الفرنسي في القانون 29 لسنة 1988 الخاص بالجرائم المعلوماتية لم يشر إلى كلمة مستند إلكتروني في مادة [5/462] الخاصة بالتزوير، وإنما استعمل التزوير في محررات معلوماتية، كما أنه أفرد نصًا للعقاب على التزوير في المستندات المعالجة آليًا، وبذلك حمى المشرع هذه المستندات لقناعته بمدى قيمتها في التعامل في كثير من المجالات، وللثقة التي يحصلها المتعاملون بها.[1]

وبعد صدور قانون العقوبات الفرنسي الجديد حذفت جريمتا تزوير المستندات المعالجة آليًا واستعمالها من بين جرائم الاعتداء على نظام المعالجة الآلية للمعطيات، وهذا الحذف له ما يبرره، وهو اختلاف المصلحة التي يحميها القانون في هاتين المجموعتين من الجرائم، فالمصلحة التي يحميها المشرع من تجريم الاعتداء على نظام المعالجة الآلية للمعطيات هي هذا النظام ذاته، أو بمعنى أدق هي مصلحة صاحب الحق في هذا النظام أو مصلحة من له السيطرة عليه، بينما المصلحة التي يحميها القانون بصدد جريمة التزوير هي الثقة العامة في المستندات ذات القيمة القانونية أيًا كان شكلها[2].

وقد جاء نص المادة [1/441] من الكتاب الرابع في قانون العقوبات الفرنسي الجديد بأنه: (يعد تزويرًا كل تغيير تدليسي للحقيقة يكون من شأنه أن يحدث ضررًا، ويقع بأي وسيلة كانت سواء وقع في محرر أو سند معبرًا عن الرأي أيًا كان موضوعه، والذي أعد مسبقًا كأداة لإنشاء حق أو ترتيب أثر قانوني معين).

---

(1) د. هدى حامد قشقوش، جرائم الحاسب الآلي، مرجع سابق، ص 123.

(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 63.

والملاحظ على هذا النص أن المشرع الفرنسي توسع في طرق التزوير، فلم تعد محددة على سبيل الحصر كالقانون الإماراتي أو المصري، وإنما أطلقها.

هذا وقد خالف أصحاب هذا الرأي القول بأن طرق التزوير واردة في القانون على سبيل الحصر، فقرروا أنه يكفي لصحة الحكم بالإدانة أن يبين كيف وقع التزوير، وليس عليه بعد ذلك أن يرد الطريقة التي وقع بها التزوير إلى واحدة من تلك الطرق التي قيل بورودها على سبيل الحصر[1].

واستندوا في رأيهم إلى أن الفقه والقضاء في مصر أضافا التقليد والاصطناع إلى طرق التزوير رغم أنهما لم يردا في المادتين (211، 213) من قانون العقوبات واللتين بينتا طرق التزوير، كما قرروا أن الثابت عملا هو وقوع التزوير بأي وسيلة يتم عن طريقها تغيير الحقيقة في محرر من المحررات، وأخيرًا فإن الفقه أضاف طريقة التزوير المعنوي وهي جعل واقعة مزورة في صورة واقعة صحيحة، وهذه الصورة لم ترد في المادة التي حددت طرق التزوير.

أما القانون رقم 2006/2 في شأن مكافحة جرائم تقنية المعلومات بدولة الإمارات فقد نص في المادة (4) منه على أن " يعاقب بالسجن المؤقت كل من زور مستندًا من مستندات الحكومة الاتحادية أو المحلية أو الهيئات أو المؤسسات العامة الاتحادية والمحلية معترفًا به قانونًا في نظام معلوماتي، وتكون العقوبة الحبس والغرامة أو إحدى هاتين العقوبتين إذا وقع التزوير فيما عدا ذلك من المستندات إذا كان من شأن ذلك إحداث ضرر، ويعاقب بالعقوبة المقررة لجريمة التزوير حسب الأحوال من استعمل المستند

---

(1) د. عبد الفتاح بيومي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 230.

المزور مع علمه بتزويره ".

ولما كان المستند الإلكتروني من المصطلحات الحديثة في المجال القانوني، فقد عرفه القانون بأنه سجل أو مستند يتم إنشاؤه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه بوسيلة إلكترونية على وسيط ملموس، أو على وسيط إلكتروني آخر، ويكون قابلا للاسترجاع بشكل يمكن فهمه.

وهذا المستند شأنه شأن باقي المستندات، أي أنه قد يكون عرضة للتزوير وتغيير الحقيقة فيه، إلا أنه يختلف عن ذلك المستند التقليدي بشقيه العرفي والرسمي والمحمي في الفصل الخامس من الباب الأول من الكتاب الثاني في قانون العقوبات الاتحادي كما سبق وأن شاهدنا، وذلك من كون أن إنشاءه أو تخزينه أو استخراجه أو نسخه أو إرساله أو إبلاغه أو استلامه يكون بوسيلة إلكترونية وعلى وسيط إلكتروني، كما اشترط القانون أن يكون هذا المستند قابلا للاسترجاع بشكل يمكن فهمه.

وتعريف التزوير السائد في الفقه هو تعريف إميل جارسون بأن التزوير في المحررات هو تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي بينها القانون تغييراً من شأنه أن يسبب ضررًا.[1]

وتزوير المستندات الإلكترونية يتم بإحدى الطرق المنصوص عليها في قانون العقوبات والسابق الإشارة إليها، كتغيير الحقيقة في هذا المستند، وذلك كأن يتم تزوير المعلومات بوضع معلومات بديلة للمعلومات الحقيقية، والتلاعب في المعطيات واستبدالها، وإتلاف بعض البيانات الموجودة بداخل المستند الإلكتروني، ولا عبرة للغة في المستند سواء أكان باللغة العربية أو

(1) جندي عبد الملك، الموسوعة الجنائية، ج4، دار الكتب المصرية، ص 361.

أية لغة أجنبية، أو أية رموز أو إشارات لها دلالتها.[1]

وحمى القانون المستند الإلكتروني من التزوير في المادة (4) منه حين فرق بين نوعين من المستندات:

النوع الأول: المستندات الخاصة بالحكومة الاتحادية، أو الهيئات أو المؤسسات العامة الاتحادية والمحلية، شريطة أن يكون هذا المستند معترفًا به قانونًا في نظام معلوماتي، أي في مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الإلكترونية أو غير ذلك، ونعتقد أن الاعتراف الذي تطلبه القانون بحق المستند مصدره هو ذات المؤسسة أو الهيئة التي أصدرته, ويقصد بذلك أن تتسم هذه المستندات بالطبيعة الإلكترونية, على سبيل المثال: بطاقات الهوية وجوازات السفر, وتصاريح الدخول, وتأشيرات الإقامة, والعقود الإلكترونية, والمستندات الموقع عليها توقيعًا إلكترونيًا[2].

والنوع الثاني من المستندات هو ما عدا ذلك من المستندات أيًا كان منشؤها أو مكان تخزينها أو استخراجها أو نسخها أو إرسالها أو إبلاغها أو استلامها، شريطة تحقق الوسيلة الإلكترونية أو الوسيط الإلكتروني، ولا تتبع المؤسسات والهيئات المذكورة في الفقرة السابقة.

ولا تقوم الجريمة إلا إذا كان من شأن هذا التزوير إحداث ضرر، وجعل

(1) سبق أن ذكرنا أن قانون العقوبات الفرنسي الجديد قد عرف التزوير في المادة 1/441 بأنه كل تغيير تدليسي للحقيقة يكون من شأنه أو من طبيعته أن يسبب ضررًا للغير, ويتم بأية وسيلة مهما كانت في محرر أو سند للتعبير عن الرأي, والذي يكون موضوعه, أو من الممكن أن يكون له أثر في إنشاء دليل على حق أو فعل تكون له نتائج قانونية.

(2) د. حسني الجندي, التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة, قانون مكافحة جرائم تقنية المعلومات, بدون ناشر, 2009, ص 20.

القانون عقوبة السجن المؤقت إذا وقع التزوير على النوع الأول من المستندات، وعقوبة الحبس والغرامة أو إحداهما إذا وقع على الثاني، وهي التفرقة ذاتها التي سار عليها المشرع في تقسيمه للمستندات في قانون العقوبات بين رسمي وعرفي.

وإن كان المشرع هنا لم يحدد طرق التزوير المعلوماتي, فإنه يمكن أن يحدث هذا التزوير بنفس الطرق المبينة في المادة (216) من قانون العقوبات الاتحادي والسابق الإشارة إليها.

وعاقب القانون في عَجُز المادة على استعمال هذا المحرر المزور بذات العقوبة المقررة لجريمة التزوير بحسب الأحوال، واشترط علم الجاني بأن هذا المستند الذي يقوم باستعماله مزور، واستعمال المحرر المزور يعني إبرازه والاحتجاج به فيما زور من أجله على اعتبار أنه صحيح.

ولا تقوم جريمة استعمال الورقة المزورة إلا بثبوت علم من استعملها بأنها مزورة، ولا يكفي مجرد التمسك بها أمام الجهة التي قدمت لها ما دام لم يثبت أنه هو الذي قام بتزويرها أو شارك في هذا الفعل أو علم بأنها مزورة[1].

ونستطيع القول بأن المشرع الإماراتي قد ساوى بين التزوير التقليدي والتزوير المعلوماتي، وبالرغم من إفراده نصوصًا خاصة للتزوير المعلوماتي، إلا أنه لم يبين طريقة هذا التزوير، وبالتالي يرجع للقواعد التقليدية المنصوص عليها في قانون العقوبات الاتحادي.

وقد نص القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها في المادة (4) منه على أن: (كل من ارتكب تزويرًا في أحد المستندات المعالجة في نظام معلوماتي يعاقب بالحبس مدة لا تقل

(1) الطعن رقم 546 لسنة 67 ق بتاريخ 2006/5/17.

عن....... ويعاقب بذات العقوبة كل من استعمل المستند المزور مع علمه بالتزوير).

والملاحظ على النص العربي أنه لم يفرق بين المستندات الرسمية والعرفية، وإنما ساوى بين جميع المستندات الإلكترونية، فتقوم الجريمة متى ما وقع تزوير على المستند الإلكتروني أيًا كان نوع هذا المستند، كما أن القانون لم يضع تعريفًا للمستند الإلكتروني المشمول بالحماية.

كما نصت الاتفاقية الأوروبية للجريمة الإلكترونية (بودابست 2001) في الفصل الثاني على الجرائم المتعلقة بالكمبيوتر في المادة (7) تحت عنوان "جريمة التزوير المتعلقة بالكمبيوتر" على أنه: (تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدًا وبغير حق: إدخال، أو تبديل، أو محو، أو تدمير بيانات كمبيوتر، ينتج عنها بيانات غير أصلية، بقصد استخدامها أو التعويل عليها في أغراض قانونية كما لو كانت أصلية، بغض النظر عما إذا كانت هذه البيانات مقروءة ومفهومة بشكل مباشر من عدمه، ويجوز لطرف أن يشترط وجود نية التدليس أو قصد غير أمين مشابه لقيام المسئولية الجنائية).[1]

---

(1) د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية، مرجع سابق، ص 16.

والنص الإنجليزي للاتفاقية:

Title 2، Computer،related offences

Article 7، Computer،related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic

والغرض من هذه المادة - كما ورد في المذكرة التفسيرية للاتفاقية - هو خلق جريمة موازية لتزوير الوثائق المادية، فهي تهدف إلى ملء الفراغ في القانون الجنائي المقرر على التزوير التقليدي، والذي يتطلب إفادة مقروءة بصريًا أو إعلانًا متضمنًا في وثيقة، وهي مادة لا يمكن تطبيقها على التخزين الإلكتروني للبيانات.

فالتلاعب بمثل هذه البيانات ذات القيمة البرهانية يمكن أن يؤدي إلى ذات النتائج الخطرة كما هو الحال في الأفعال التقليدية للتزوير إذا قام طرف ثالث بالوقوع في التضليل أو الخداع الناجم عنها، حيث يشمل التزوير باستخدام الحاسوب إعدادًا غير مصرح به أو تعديلا في بيانات مخزنة، بحيث تتضمن قيمة برهانية مختلفة في إطار المعاملات التي تعتمد على مصداقية المعلومة التي تحتوي عليها البيانات، وهذا هو محل التضليل، والمصلحة المشمولة بالحماية القانونية هنا هي الأمن والثقة في البيانات المخزنة التي يمكن أن تؤثر في العلاقات القانونية.[1]

ويجب ملاحظة أن مفهوم التزوير يختلف كثيرًا من دولة إلى أخرى، فهناك مفهوم يكون مؤسسًا على الصحة بالنسبة لكاتب الوثيقة، في حين أن بعض المفاهيم الأخرى ترتكز على صدق المعلومات المتضمنة في الوثيقة محل البحث.[2]

---

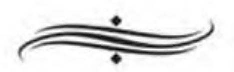
data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

(1) د. عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية، مرجع سابق، ص 85.

(2) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص 97.

وعلى الرغم من ذلك فإنه قد تم الاتفاق على أن التضليل المستند إلى المصداقية يشير في الحد الأدنى إلى واضع البيانات بصرف النظر عن صحة أو انضباط مضمون البيانات، ويمكن للأطراف في هذه الاتفاقية الذهاب إلى أبعد من ذلك، وتضمين ذلك تحت مصطلح (مصداقية الأصالة في البيانات).[1]

وهذا النص ينطبق على البيانات المعدلة للمحرر العام أو الخاص، واللذان لهما آثار قانونية، وعلى ذلك فإن الإدخال غير المصرح به للبيانات الصحيحة وغير الصحيحة يخلق موقفًا يناظر عمل محرر مزور، كذلك فإن العمليات اللاحقة للإتلاف كالتعديلات أو التغييرات الجزئية والمحو كواقعة خروج البيانات الممثلة على دعامة، والطمس كواقعة حفظ وإخفاء بيانات، كل أولئك يناظر بشكل عام تزوير محرر صحيح.[2]



(1) د. عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية، مرجع سابق، ص 86.

(2) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص 99.

المبحث الرابع

جريمة الاحتيال والنصب الإلكتروني

يحمي القانون الجنائي حق الملكية سواء أكان محله عقارًا أم منقولا، وإن كانت ملكية المنقولات تحظى بالنصيب الأوفر من رعاية التشريع الجنائي.

والجرائم التي تقع اعتداءً على ملكية المنقول تنقسم إلى طائفتين رئيسيتين، الأولى تضم جرائم تكون الغاية منها الاستيلاء على مال الغير، والأخرى تشمل جرائم تكون غايتها إتلاف مال الغير، ويدخل ضمن الطائفة الأولى جرائم السرقة والاحتيال والنصب وخيانة الأمانة[1]، وسوف نتناول في هذا المبحث جريمة الاحتيال والنصب[2] والتي اتخذت مع الزمن صورًا متعددة، وتنوعت أساليب المحتالين ونشطت وسائلهم، وبالأخص في نطاق الشركات الوهمية، والتلاعب في عقود التأمين، وقيمة العملة، وعمليات البنوك، وبوجه عام في أمور البيع والشراء، حتى لقد اضطر القضاء إلى التوسع في أحوال العقاب توسعًا كبيرًا حماية لمصالح الجماهير، والتي هي بطبيعتها سهلة التصديق سريعة الانقياد، وهو ما جعل النصب يشمل أغلب صور التدليس المدني.[3]

(1) د. عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 408 وما بعدها.

(2) محمد محرم محمد علي، جريمة النصب والتجارة لإلكترونية، بحث منشور على شبكة الإنترنت على الموقع:
http://www.arablaw.org/Research%20&%20Studys.htm

(3) د. رءوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، القاهرة، 1978، ص 449.

وقد أوردت قوانين العقوبات جريمة النصب إلى جانب جريمة خيانة الأمانة، وإعطاء شيك لا يقابله رصيد، والإقراض بربا فاحش، وقد جاء النص عليه في القانون الروماني والقانون الفرنسي القديم مختلطًا بالسرقة، بل إنه لم يبرز كجريمة مستقلة بذاتها إلا بعد قيام الثورة الفرنسية، فوضع المشرع الفرنسي نصًا خاصًا بجريمة النصب في قانون العقوبات الصادر 1791 ثم في تشريع 1810، وكان يعبر عنه في هذين التشريعين بلفظ التدليس[1]، وسوف نتناول جريمة النصب من خلال بيان أركان جريمة النصب، ثم بحث مدى احتمال طبيعة التجارة الإلكترونية لأن تكون محلا للاعتداء بالسرقة أو النصب أو خيانة الأمانة، وبمعنى آخر هل الأموال المتداولة في نطاق التجارة الإلكترونية تحتمل أن تكون محلا للسرقة أو النصب أو خيانة الأمانة؟

لذلك تم تقسيم هذا المبحث إلى مطلبين كما يلي:

المطلب الأول: أركان جريمة النصب.

المطلب الثاني: حماية أموال التجارة الإلكترونية من خلال القواعد العامة لجريمة النصب.

(1) د. رءوف عبيد، جرائم الاعتداء على الأشخاص والأموال، مرجع سابق، ص 449.
وانظر أيضا: د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، 1992.

المطلب الأول

أركان جريمة النصب

تناول المشرع في دولة الإمارات العربية المتحدة جريمة النصب والاحتيال في المادة (339) من قانون العقوبات الاتحادي، التي نصت على أنه:

"يعاقب بالحبس أو بالغرامة كل من توصل إلى الاستيلاء لنفسه أو لغيره على مال منقول، أو سند، أو توقيع هذا السند، أو إلى إلغائه أو إتلافه أو تعديله، وذلك بالاستعانة بطريقة احتيالية، أو باتخاذ اسم كاذب أو صفة غير صحيحة، متى كان من شأن ذلك خداع المجني عليه وحمله على التسليم، ويعاقب بالعقوبة ذاتها كل من قام بالتصرف في عقار أو منقول يعلم أنه غير مملوك له، أو ليس له حق التصرف فيه، أو تصرف في شيء من ذلك مع علمه بسبق تصرفه فيه أو التعاقد عليه، وكان من شأنه الإضرار بغيره، وإذا كان محل الجريمة مالا أو سندا للدولة أو لإحدى الجهات التي ورد ذكرها في المادة (5) عد ذلك ظرفًا مشددًا، ويعاقب على الشروع بالحبس مدة لا تجاوز سنتين، أو بالغرامة التي لا تزيد على عشرين ألف درهم، ويجوز عند الحكم على العائد بالحبس مدة سنة فأكثر أن يحكم بالمراقبة مدة لا تزيد على سنتين ولا تجاوز مدة العقوبة المحكوم بها".

كما تناول المشرع المصري جريمة النصب في المادة (336) عقوبات مصري والتي جاء نصها: [يعاقب بالحبس وبغرامة لا تتجاوز خمسين جنيهًا مصريًا أو بإحدى هاتين العقوبتين فقط كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات مخالصة أو أي متاع منقول، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها، إما باستعمال طرق احتيالية من

شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة، أو إحداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الاحتيال، أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور، وإما بالتصرف في مال ثابت أو منقول ليس ملكًا له ولا له حق التصرف فيه، وإما باتخاذ اسم كاذب أو صفة غير صحيحة، أما من شرع في النصب ولم يتممه فيعاقب بالحبس مدة لا تتجاوز سنة، أو بغرامة لا تتجاوز عشرين جنيهًا مصريًا، ويجوز جعل الجاني في حالة العود تحت ملاحظة البوليس مدة سنة على الأقل وسنتين على الأكثر].

والاحتيال أو النصب هو الاستيلاء على الحيازة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسلم ذلك المال[1]، أو أنه الاستيلاء على مال منقول مملوك للغير بخداع المجني عليه وحمله على تسليمه.[2]

ويجري الفقه في هذا الصدد التفرقة بين استغلال سرعة التصديق في مواجهة شخص دون سبك وبين التوصل إلى التصديق بالحبك والنسج لما يخالف الحقيقة بغية الإيقاع في الغلط.[3]

وتتكون جريمة الاحتيال من ثلاثة أركان، أولها: الركن المادي وهو

(1) نقض 12 مايو سنة 1952، مجموعة أحكام محكمة النقض المصرية، س 3، ص 915.
(2) كما عرفه البعض بأنه الاستيلاء على الحيازة الكاملة عمدا بطريق الحيلة أو الخداع على مال مملوك للغير، راجع في ذلك: د. حسن صادق المرصفاوي، قانون العقوبات الخاص، منشأة المعارف، الإسكندرية، 1991، ص 394، د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 990، د. عوض محمد عوض، جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية، 1984، ص 356.
(3) د. عبد المهيمن بكر سالم، جرائم الاعتداء على الأشخاص والأموال، 1977، ص437.

وسيلة الاحتيال، والثاني: محل الجريمة أو موضوعها، والثالث: القصد الجنائي، ونتناول فيما يلي الأركان الثلاثة من خلال ثلاثة فروع.

الفرع الأول

الركن المادي

يعرف الركن المادي في جريمة الاحتيال أو النصب بأنه الوسيلة التي يلجأ إليها الجاني في سبيل تحقيق الغرض الذي يرمي إليه، وهو الاستيلاء لنفسه أو لغيره على مال منقول، أو سند أو توقيع على هذا السند، أو إلغاؤه أو إتلافه أو تعديله، كما يعد من وسائل الاحتيال التصرف في عقار أو منقول غير مملوك للجاني، فوسيلة الاحتيال إذن إما أن تكون بالاستعانة بطريقة احتيالية أو باتخاذ اسم كاذب أو صفة غير صحيحة، وإما أن تكون بالتصرف في عقار أو منقول، ويتكون الركن المادي من ثلاثة عناصر، هي وسائل التدليس المنصوص عليها في القانون على سبيل الحصر، والنتيجة التي تترتب على هذا النشاط وهي تسليم المجني عليه ماله إلى الجاني، وتوافر علاقة السببية بين هذا النشاط وتلك النتيجة، بمعنى أن يكون تسليم المال إلى الجاني قد وقع نتيجة لوسيلة التدليس التي استخدمها، وقد حدد المشرع الإماراتي هذه الوسائل على سبيل الحصر في المادة (399) عقوبات كما حددها المشرع المصري في المادة (336) عقوبات، وهي:

1) استعمال طرق احتيالية.

2) التصرف في مال غير مملوك للجاني وليس له حق التصرف فيه.

3) اتخاذ اسم كاذب أو صفة غير صحيحة.

ويشترط في الاستعانة بأي من هذه الوسائل أن يكون من شأن ذلك خداع المجني عليه وحمله على تسليم المال المنقول أو السند أو التوقيع عليه

أو إلغائه أو إتلافه أو تعديله.

الطرق الاحتيالية:

وتعرف بأنها ادعاءات كاذبة يدعمها الجاني بمظاهر خارجية من شأنها إيهام المجني عليه بأمر من الأمور التي نص عليها القانون، ولاعتبار ما صدر من الجاني طرقًا احتيالية يجب أن يتوافر فيها ثلاثة شروط:

1) أن تنطوي على ادعاء كاذب.

2) أن يدعم الجاني هذا الادعاء بمظاهر خارجية.

3) أن يكون من شأن هذا الادعاء إيهام المجني عليه بأمر من الأمور التي نص عليها القانون[1].

وقد قضي بأن جريمة النصب كما هي معروفة في القانون يتعين لتوافرها أن يكون ثمة احتيال وقع على المجني عليه بقصد خداعه والاستيلاء على ماله، كما تقع جريمة النصب بطريقة الاستعانة بشخص آخر لتأييد الأقوال والادعاءات المكذوبة، على أن يكون تدخل هذا الشخص الآخر بسعي من الجاني وتدبيره وإرادته، كذا تقوم جريمة النصب باتخاذ صفة غير صحيحة إذ تكفي وحدها لقيام ركن الاحتيال.[2]

ومن المسلم به فقهًا وقضاءً أن الكذب المجرد لا يكفي لتوافر الطريقة الاحتيالية، مهما كان منمقا مرتبًا يوحي بتصديقه، ومهما تكررت وتنوعت

(1) د. رءوف عبيد، جرائم الاعتداء على الأشخاص والأموال، مرجع سابق، ص568, وفي المعنى ذاته: د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 990, ومحمد محرم محمد علي، خالد محمد كدفور المهيري، قانون العقوبات الاتحادي، الفتح للطباعة والنشر، 1992، ص 1098.

(2) حكم محكمة تمييز دبي، بتاريخ 19 /1 / 2009 في الطعن رقم 2008 / 437 جزاء.

صيغه، وقد قضت محكمة النقض بأن جريمة النصب لا تتحقق بمجرد الأقوال والادعاءات الكاذبة ولو كان قائلها قد بالغ في توكيد صحتها حتى تأثر بها المجني عليه، بل يجب أن يكون قد اصطحب بأعمال مادية أو مظاهر خارجية تحمل المجني عليه على الاعتقاد بصحته[1].

ومن المقرر أن استعانة المتهم بشخص آخر لتأييد أقواله وادعاءاته المكذوبة وتدخل الأخير لتدعيم مزاعمه تُعد من قبيل الأعمال الخارجية التي تساعد على حمل المجني عليه على تصديق تلك الادعاءات، وبهذه الأعمال الخارجية يرقى الكذب إلى مرتبة الطرق الاحتيالية الواجب تحققها في جريمة النصب.[2]

ويتعين إذن حتى تتوفر الطريقة الاحتيالية أن يوجد إلى جوار الكذب ما يؤيده ويوحي بصدقه، فتعمل الأكاذيب أثرها في استسلام المجني عليه، وتحمله على التسليم والتخلي عن حيازة المال موضوع الجريمة[3].

ويلاحظ أن المشرع لم يحدد في النص ماهية الطريقة الاحتيالية أو نوعها أو أسلوبها حتى تعتبر وسيلة من وسائل الاحتيال، وهو في ذلك يتوسع في الأفعال التي تعتبر طرقًا احتيالية بغرض الاستيلاء على مال الغير، ومهما يكن من أمر الطريقة الاحتيالية ونوعها وأسلوبها، فإنه يجب أن يكون من شأنها خداع المجني عليه وحمله على التسليم، على أنه يجب أن تكون الطريقة الاحتيالية على درجة من الحبك الذي يسمح بخداع الشخص متوسط الذكاء، ومع ذلك فإنه من يتوسم فيه الجاني الطيبة

(1) نقض 1985/2/21، مجموعة الأحكام، س 34 ق 48.
(2) حكم محكمة تمييز دبي، بتاريخ 19 /11 / 1994 في الطعن رقم 1994 / 93 جزاء.
(3) نقض في 1975/1/19، مجموعة الأحكام، س 26، ق 12.

والسذاجة يكون محلا للحماية القانونية، غير أنه يجب ألا يكون المجني عليه من السذاجة والغفلة لدرجة أن يصدق كل ما يقال له من أكاذيب مهما كانت فاضحة أو مكشوفة في كذبها.

ويجب أن توجه الطريقة الاحتيالية إلى المجني عليه ذاته لخداعه وغشه ابتغاء اغتيال ماله، وقد قضت محكمة النقض المصرية بأن الطرق الاحتيالية التي بينها القانون يجب توجيهها إلى خداع المجني عليه وغشه.(1)

والطرق الاحتيالية تكاد لا تدخل تحت حصر، ولكن المهم فيها أن يكون من شأنها خداع المجني عليه وحمله على تسليم المال.

وقضت محكمة النقض المصرية أنه من المقرر أن جريمة النصب كما هي معرفة به في المادة 336 من قانون العقوبات تتطلب لتوافرها أن يكون ثمة احتيال وقع من المتهم على المجني عليه بقصد خداعه والاستيلاء على ماله، فيقع المجني عليه ضحية الاحتيال الذي يتوافر باستعمال طرق احتيالية أو باتخاذ اسم كاذب أو انتحال صفة غير صحيحة أو بالتصرف في مال الغير ممن لا يملك التصرف(2).

كما قررت المحكمة أن الطرق الاحتيالية في جريمة النصب يجب أن يكون من شأنها الإيهام بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول مشروع وهمي أو غير ذلك من الأمور المبينة على سبيل الحصر في القانون(3).

اتخاذ اسم كاذب أو صفة غير صحيحة:

كذلك من وسائل الاحتيال اتخاذ الجاني اسمًا كاذبًا أو صفة غير

(1) نقض في 1963/10/14، أحكام النقض، س 14 ق 113.

(2) الطعن رقم 14039 لسنة 63 ق بتاريخ 1997/5/11.

(3) الطعن رقم 9651 لسنة 63 ق بتاريخ 1997/12/15.

صحيحة، وهذه وسيلة مستقلة بذاتها من وسائل النصب والاحتيال، وتكفي وحدها في تكوين الركن المادي في الجريمة دون حاجة لاستعمال طرق احتيالية، فيكفي لتكوين جريمة النصب أن يتسمى الجاني باسم كاذب يتوصل به إلى تحقيق غرضه دون حاجة إلى الاستعانة على إتمام جريمته بأساليب احتيالية أخرى[1]، وكذلك الحكم النسبة لانتحال صفة غير صحيحة، فمن يدعي كذبًا أنه وكيل عن شخص آخر، ويتمكن باتخاذ هذه الصفة غير الصحيحة من الاستيلاء على مال المجني عليه لتوصيله إلى موكله المزعوم يعد مرتكبًا لجريمة الاحتيال باتخاذ صفة كاذبة ولو لم يكن هذا الادعاء مقرونًا بطرق احتيالية.[2]

إلا أنه يشترط في الالتجاء إلى هذه الوسيلة من وسائل الاحتيال أن يكون من شأنها خداع المجني عليه وحمله على التسليم، فمتى كانت الواقعة هي أن المتهم لم يتجاوز في فعلته اتخاذ اسم كاذب دون أن يعمل على تثبيت اعتقاد المجني عليه بصحة ما زعمه وأن المجني عليه اقتنع به لأول وهلة، فإن ذلك لا يكون من المتهم إلا مجرد كذب لا يتوافر معه المعنى المقصود قانونًا من اتخاذ الاسم الكاذب في النصب، ذلك أن القانون وإن كان لا يقتضي أن يصحب اتخاذ الاسم الكاذب طرق احتيالية، إلا أنه يستلزم أن تحف به ظروف واعتبارات أخرى يكون من شأنها خداع المجني عليه وحمله على تصديق المتهم، وتقدير هذه الظروف والاعتبارات من شأن قاضي الموضوع[3].

(1) نقض في 1955/10/24، قضاء النقض، ق 878.
(2) نقض في 1943/2/1، مجموعة القواعد القانونية، ج6، ق 93، نقض في 1974/2/14، أحكام النقض، س 25، ق 41.
(3) نقض في 1948/2/9، مجموعة القواعد القانونية، ج7، ق 532

وكذلك إذا ادعى شخص أنه مخبر في الشرطة واستولى بهذا الادعاء على مبلغ من شخص آخر بدون أن يقترن ادعاؤه بأفعال مادية أخرى من شأنها التأثير في المجني عليه، فإن مجرد هذا الادعاء الكاذب لا يكفي لتكوين جريمة النصب، إذ ليس في مجرد اتخاذ ذلك الشخص لصفة المخبر في الشرطة ما يحمل المجني عليه على التسليم وإعطائه مالا[1]، وهذا يتفق مع ما نصت عليه المادة 399 عقوبات من أنه يجب أن يكون من شأن اتخاذ الاسم الكاذب أو الصفة غير الصحيحة خداع المجني عليه وحمله على تسليم المال، أي يجب أن يكون اتخاذ ذلك الاسم أو تلك الصفة هو السبب الذي حمل المجني عليه على تسليم المال تحت إيهامه، فإذا كان الاسم الذي تسمى به الجاني أو الصفة التي ادعاها غير ذات أثر على المجني عليه ومع ذلك قام بتسليم المال إلى الجاني فلا تتوافر في هذه الحالة جريمة الاحتيال.[2]

ويستوي في الاسم الكاذب أو الصفة غير الصحيحة كوسيلة للاحتيال أن يكون شفاهة أو يتخذه الجاني محررًا، ويستوي أن يكون الاسم المنتحل خياليًا أصلا أو حقيقيًا لشخص آخر غير الجاني، غير أن التسمي باسم الشهرة لا يعد اسمًا كاذبًا.

(1) نقض في 1930/4/17، قضاء النقض، ق 875.

(2) د. حسن المرصفاوي، قانون العقوبات الخاص، مرجع سابق، ص 250، ويرى بعض الشراح أن مجرد اتخاذ الاسم الكاذب أو الصفة غير الصحيحة يكفي في ذاته لتوفر وسيلة الاحتيال دون أي اشتراط آخر لاسيما وأنه ليس في مقدور الشخص أن يلجأ إلى سبيل يتحقق به من صدق ما يزعمه الجاني من اسم كاذب أو صفة غير صحيحة، فلم يجر العرف إذا تقدم شخص لآخر على أنه فلان أن يطلب منه تقديم بطاقته الشخصية مثلا، وكذلك من يزعم أنه محام أو طبيب لا يسأل عن الشهادة الجامعية التي نالها للاطلاع عليها.

أما الصفة غير الصحيحة فلا تقع تحت حصر، فقد تكون هذه الصفة درجة علمية، وقد تكون مهنة أو عملا يزعم الجاني الاشتغال به كاتخاذ المتهم صفة تاجر وحصوله بناءً على ذلك على بضاعة.

التصرف في مال ثابت أو منقول:

أما الوسيلة الأخرى من وسائل الاحتيال فهي التصرف في عقار أو منقول غير مملوك للجاني وليس له حق التصرف فيه، أو التصرف في شيء من ذلك مع علم الجاني بسبق تصرفه فيه أو التعاقد عليه، وهذه الوسيلة تقوم مستقلة بذاتها، ويكفي مجرد توفرها لقيام الركن المادي في جريمة الاحتيال دون اشتراط تأييدها بأشياء أخرى خارجية[1]، فزعم الجاني ملكية المال أو أن له حق التصرف فيه، أو التصرف فيه مع علمه بسبق تصرفه فيه، هو في ذاته كاف لتحقيق الركن المادي في جريمة النصب، ويشترط لتوفر هذه الوسيلة من وسائل الاحتيال أمران: الأول: التصرف في عقار أو منقول، والثاني: أن يكون هذا المال غير مملوك للجاني وليس له حق التصرف فيه، أو سبق أن تصرف فيه.

ويقصد بالتصرف في عقار أو منقول هنا كل تصرف ناقل للملكية كالبيع والمقايضة والهبة، أو كل تصرف يقرر على العقار حقا عينيًا كحق الارتفاق أو الرهن[2]، أما التأجير فلا يعد تصرفًا في جريمة النصب، ويستوي أن يكون محل التصرف عقارا أو منقولا، فإذا كان التصرف بالبيع مثلا واردًا على عقار فإن المجني عليه هو المتصرف إليه الذي يسلم المال للجاني، وتقوم وسيلة الاحتيال في هذه الحالة دون أية شبهة.

(1) نقض في 1949/2/9، مجموعة الأحكام، س 1، ق 56.

(2) نقض في 1960/1/22، مجموعة الأحكام، س 17، ق 24، نقض في 1936/6/15، مجموعة القواعد القانونية، ج 3، ق 484.

أما إذا كان محل التصرف منقولا، وكان هذا المنقول معينًا بالنوع كصنف معين من الحبوب أو الثمار، فإن العقد يتم بمجرد تلاقي الإيجاب والقبول بغير توقف على تسليم المبيع، فإن كانت نية الجاني هي الاستيلاء على المال ولم ينصرف قصده إلى تسليم المنقول المعين بالنوع كان فعله هذا مكونًا للركن المادي في جريمة الاحتيال، أما إذا كانت نية الجاني هي تسليم المنقول فعلا ولم يكن منتويًا اغتيال مال فلا يتوافر في حقه الركن المادي في جريمة النصب حتى ولو عجز بعد هذا عن تسليم المبيع.

أما إذا كان محل التصرف معينًا بالذات كسيارة أو دابة محددة بأوصافها، فإن جريمة الاحتيال تقوم بتمكين الجاني من الاستيلاء على مال المجني عليه، فمن يشاهد سيارة ويتوجه إلى الجاني معتقدًا أنه مالكها يبغي شراءها منه، فيبدي هذا الأخير استعداده لبيعها له مؤكدًا أنها ملكه، ويتفق معه على تسليمها إليه بعد تحرير عقد البيع وقبض الثمن، فإذا تم هذا واختفى الجاني قبل التسليم عد مرتكبًا لجريمة النصب.

ويجب أن يكون المال غير مملوك للجاني وليس له حق التصرف فيه، أو تصرف فيه مع علمه بسبق تصرفه فيه، فإن كان مملوكًا له أو له حق التصرف فيه فلا جريمة، فالوكيل الذي يقوم بالتصرف في مال مملوك لموكله بناءً على عقد وكالة يفوضه فيه بالبيع لا يرتكب جريمة نصب حتى ولو ظهر بعد ذلك أن الوكالة كانت قد انتهت أو انقضت ولم يكن الوكيل قد علم بذلك.

وكذلك يتوفر الركن المادي لجريمة النصب أو الاحتيال في حالة تصرف الجاني في المال مرتين، ويكون المجني عليه في هذه الحالة المتصرف إليه الثاني، أما المتصرف إليه الأول فليس هناك جريمة نصب وقعت في حقه.

على أنه يشترط بداهة أن يجهل المجني عليه أن المال ليس في ملكية الجاني، أو أنه ليس له حق التصرف فيه، أو أنه قد سبق التصرف فيه، وإلا فلا جريمة، وقد قضي بأنه إذا كان دفاع المتهم قوامه عدم توافر عنصر الاحتيال في الدعوى لأن المجني عليه حين تعاقد معه كان يعلم أنه غير مالك لما تعاقد معه عليه، فإن الحكم إذ أدانه في جريمة النصب على أساس أن التصرف في مال لا يملكه المتهم، واعتبار ذلك طريقة من طرق النصب قائمة بذاتها، ولا يشترط فيها وجود طرق احتيالية، ويكون بالتالي قاصر البيان في الأسباب التي بني عليها.[1]

الفرع الثاني

محل الجريمة أو موضوع الاحتيال

يشترط أن يكون موضوع جريمة الاحتيال أو النصب مالا منقولا أو عقارًا مملوكًا لغير الجاني وليس له حق في التصرف فيه، أو تصرف فيه مع علمه بسبق تصرفه فيه.

ولا أهمية لقيمة المال - عقارًا كان أم منقولا - في قيام جريمة الاحتيال، كذلك لا عبرة بكون المال له قيمة مادية أو مجرد قيمة أدبية كالخطابات والمذكرات الخاصة[2]. ويستوي في المال موضوع الجريمة أن تكون حيازة المجني عليه له مشروعة أو غير مشروعة، فمن يتوصل بالاحتيال إلى الاستيلاء على مواد مخدرة من آخر يعد مرتكبًا لجريمة النصب إذا توافرت أركانها، وكذلك الحال فيمن يستولي على سلاح غير

(1) نقض في 1944/12/11، مجموعة القواعد القانونية، ج 6، ق 420، نقض في 1966/5/16، مجموعة أحكام النقض، س 17، قاعدة رقم 114.

(2) د. حسن المرصفاوي، قانون العقوبات الخاص، مرجع سابق، ص 433.

مرخص بحيازته.[3]

ونشير هنا إلى أن الاستيلاء على المنفعة فقط بإحدى وسائل الاحتيال لا يكفي لقيام محل جريمة النصب، كمن يتوصل بطريق الحيلة إلى الركوب في وسائل المواصلات العامة بغير أجر تحت الزعم بأنه من رجال الشرطة مثلا.

والعبرة في ملكية المال المنقول أو العقار للجاني أو عدم ملكيته إياه هي بالحقيقة والواقع، فإذا كان المال مملوكًا لمن استولى عليه فلا جريمة في الأمر حتى ولو كان يعتقد وقت استيلائه على المال أنه مملوك لغيره، فإذا كان المال في ملك من يحتال لأخذه وهو يعلم بملكيته له وقد التجأ إلى هذه الوسيلة في سبيل الحصول عليه فلا جريمة يمكن إسنادها إليه[1].

إلا أنه يشترط في الاستيلاء على المال بأي وسيلة من وسائل الاحتيال المشار إليها آنفًا أن يكون من شأن ذلك الإضرار بالغير، أي أن يلحق بالمجني عليه ضرر من استيلاء الجاني على ماله؛ لأنه ما لم يحصل أي ضرر فلا يكون هناك سلب لمال الغير، ويؤخذ من أحكام محكمة النقض المصرية أنها تشترط الضرر ولو كان محتملا، فقد قضت بأن مجرد الاستيلاء على نقود عن طريق التصرف في مال ثابت أو منقول ليس ملكًا للمتصرف ولا له حق التصرف فيه يعتبر نصبًا معاقبًا عليه، بغض النظر عما إذا كان الضرر الحاصل من هذا التصرف قد وقع فعلا على الطرف الآخر في العقد أو على صاحب الشيء الواقع فيه التصرف[2]، كما قضت أيضًا بأنه يكفي لتحقيق جريمة النصب أن يكون الضرر محتمل الوقوع[3].

(1) د. حسن المرصفاوي، قانون العقوبات الخاص، مرجع سابق، ص 435.
(2) نقض في 1936/6/8، مجموعة القواعد، ج 3، ق 481.
(3) نقض في 1945/12/10، مجموعة القواعد القانونية، ج 7، ق 39.

الفرع الثالث

القصد الجنائي

جريمة الاحتيال أو النصب جريمة عمدية تتطلب توفر القصد الجنائي العام والقصد الخاص، ويتوفر القصد الجنائي العام فيها بعلم الجاني بأن الأفعال التي يأتيها يعدها القانون وسائل احتيال، ومن شأنها خداع المجني عليه وحمله على تسليم المال، أما القصد الخاص فيتمثل في انصراف نية الجاني إلى الاستيلاء على الحيازة الكاملة لمال المجني عليه.

فمن يتصرف في منقول أو عقار معتقدًا أنه أصبح مملوكًا له بطريق الميراث وهو لم يرثه بعد، لا تتوافر في حقه جريمة الاحتيال لتخلف القصد الجنائي العام، كذلك إذا لم يكن قصد الجاني منصرفًا إلى تملك المال الذي تحصل عليه من حائزه بطريقة الحيلة انتفى قيام القصد الجنائي الخاص، وانتفت بالتالي جريمة النصب، فمن يتوصل بوسائل الاحتيال إلى الحصول على منفعة مال من آخر لا يعد مرتكبًا لجريمة النصب؛ لأن العبرة هي نية الجاني في الاستيلاء على مال المجني عليه، لا مجرد الحصول على منفعة هذا المال، إلا أنه يشترط أن يتعاصر القصد الجنائي العام والخاص في جريمة الاحتيال مع وقت الاستيلاء على المنقول أو العقار، وقيام القصد الجنائي بشقيه عند الجاني مرده إلى وقائع الدعوى وما تستخلصه منها محكمة الموضوع، ولا عبرة في توفره بالباعث الذي دفع الجاني إلى ارتكاب الجريمة.

وقد نصت الفقرة الثانية من المادة 399 عقوبات على ظرف مشدد في جريمة النصب، وهو إذا ما كان محل الجريمة مالا أو سندًا للدولة، أو لإحدى الجهات التي ورد ذكرها في المادة الخامسة عقوبات ومنها

الوزارات والدوائر الحكومية والهيئات والمؤسسات العامة والجمعيات والمؤسسات ذات النفع العام، والحكمة من تشديد العقوبة في مثل هذه الأحوال هي الحفاظ على أموال تلك الجهات، فضلا عما يتسم به عمل الجاني من جرأة وجسارة تتمثل في الاستيلاء لنفسه أو لغيره على مال للدولة بإحدى وسائل النصب والاحتيال.

وجريمة النصب والاحتيال من الجنح التي يعاقب القانون على الشروع فيها، ويتوافر الشروع في هذه الجريمة إذا أتى الجاني وسيلة من وسائل الاحتيال للاستيلاء على مال المجني عليه، فاكتشف هذا الأخير تلك الوسيلة ولم ينخدع ويسلمه المال، أو لم يكتشف المجني عليه هذه الوسيلة ولكن الجريمة ضبطت وقت تسليم المال.

وغني عن البيان أن الطريقة الاحتيالية هي من العناصر الأساسية الداخلة في تكوين الركن المادي لجريمة النصب، وبالتالي فإن استعمال الجاني إياها يعد شروعًا في الجريمة باعتبارها من الأعمال التنفيذية[1]، أما الدجال الذي يؤثث مكانًا على شكل عيادة طبية، ويعين فيها ممرضًا فإن أعماله هذه تعد أعمالا تحضيرية لجريمة النصب لا عقاب عليها[2].

وقد عاقب المشرع الإماراتي على الشروع في جريمة النصب في المادة 3/399 بعقوبة الحبس مدة لا تجاوز سنتين، أو الغرامة التي لا تزيد على عشرين ألف درهم.

وفضلا عن حق القاضي في تشديد عقوبة النصب في حالة المتهم العائد والحكم عليه بالحبس مدة سنة فأكثر، فقد أجاز له المشرع أن يحكم بوضع

(1) نقض في 1971/6/20، مجموعة الأحكام، س 22، ق 118، نقض في 1972/5/29 مجموعة الأحكام، س 23، ق 192.

(2) د. حسن المرصفاوي، قانون العقوبات الخاص، مرجع سابق، ص 442.

الجاني تحت مراقبة الشرطة مدة لا تزيد على سنتين ولا تجاوز مدة العقوبة المحكوم بها، ويجب أن يبين في الحكم يوم بدء المراقبة.

ويصح الحكم بالمراقبة سواء أكانت الجريمة تامة أم مجرد شروع فيها لإطلاق النص[1].

المطلب الثاني

حماية أموال التجارة الإلكترونية

من خلال القواعد العامة لجريمة النصب

سهلت شبكة الإنترنت ارتكاب جرائم النصب والخداع لسببين:

الأول هو طغيان واستحواذ الوضع الاقتصادي على الفرد، واعتقاده أنه يمكنه القيام بتحسين ظروفه الاقتصادية عبر اقتراح الأفكار أو استقبالها من خلال شبكة الإنترنت، وذلك كأثر للإبهار الذي تركته شبكة الإنترنت في عقول المتعاملين بها.

الثاني ما تسمح به شبكة الإنترنت من اختراق المحظور؛ نظرًا لأن استخدامها مفتوح للجميع دون وجود ما يقيد حركتها أو الحركة عبرها باعتبارها أداة تواصلية مشروعة.

ويضاف إلى ذلك أن العالم الافتراضي بطبيعته يعد أسلوبًا فنيًا يسهل قيام جريمة النصب؛ لأن له مدلولا أعمق وأوسع تأثيرًا في المجني عليه، فيمكن عبر شبكة الإنترنت اتخاذ اسم كاذب، أو صفة غير صحيحة، أو إقامة مشروع وهمي، أو واقعه مزورة، أو إحداث الأمل بربح، أو إعداد سندات مالية غير صحيحة، وهذه كلها وقائع مكونة لجريمة النصب.

(1) د. رءوف عبيد، شرح قانون العقوبات، القسم الخاص " الاعتداء على الأشخاص والأموال"، مرجع سابق، ص 499.

ويدور التساؤل: هل الأموال المتداولة في نطاق التجارة الإلكترونية تحتمل أن تكون محلا للسرقة أو النصب أو خيانة الأمانة؟ وسوف نبين في هذا المطلب مدى صلاحية المال المعلوماتي أن يكون محلا لجريمة النصب في فرع أول، والحماية التي يسبغها تجريم النصب على أموال التجارة الإلكترونية في فرع ثان.

الفرع الأول

مدى صلاحية المال المعلوماتي أن يكون محلا لجريمة النصب

الاحتيال لا يقع على الشخص الطبيعي فقط، بل إنه من المسلم به صلاحية الشخص المعنوي لاعتباره مجنيًا عليه، فالشركات والمؤسسات العامة والخاصة هي من الأشخاص الاعتبارية في نظر القانون، وحيث إن الحاسوب والشبكات الداخلية للمنشأة تعد من فروع الشركة أو المؤسسة، فإنها قد تكون صالحة لوقوع فعل الخداع أو التحايل عليها.[1]

وطالما أن القانون أضفى الحماية الجنائية على الأشخاص الاعتبارية بجانب الأشخاص الطبيعيين، فإن التساؤل يثور حول إمكانية ممارسة أفعال الاحتيال على الحاسب الآلي وإيقاعه في الغلط، وبالتالي إمكانية تطبيق النصوص الجنائية القائمة الخاصة بجريمة النصب على هذا النوع من الاحتيال.

هناك ثلاثة اتجاهات: الأول يرى أن جريمة النصب لا تقوم إلا إذا خدع شخص شخصًا مثله، وأن يكون الشخص المخدوع مكلفًا بمراقبة البيانات، وعلى ذلك لا يتصور خداع الحاسب الآلي بوصفه آلة، ومن ثم لا يطبق النص الجنائي الخاص بالنصب والاحتيال لافتقاره أحد العناصر اللازمة

(1) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، مرجع سابق، ص 185.

لتطبيقه، وهذا الاتجاه تتبناه تشريعات مصر وألمانيا والدانمارك وفنلندا واليابان والنرويج والسويد ولكسمبرج وإيطاليا.[1]

والاتجاه الثاني: وتتبناه الدول الأنجلوسكسونية ومنها بريطانيا وأستراليا وكندا، وهو اتجاه يوسع من نطاق تطبيق النصوص المتعلقة بالعقاب على جريمة النصب[2]، ويسمح بتطبيق هذه النصوص على النصب المعلوماتي، ولقد تدخل المشرع الإنجليزي عام 1983 واعتبر خداع الآلة بنية ارتكاب غش مالي هو من قبيل الاحتيال الذي يجب العقاب عليه جنائيًّا، وبذلك تطبق نصوص تجريم النصب على ذلك الغش أو الاحتيال بطرق معلوماتية، ولقد سار على ذلك النهج القضاء الكندي والأسترالي.[3]

كما يرى جانب من الفقه الفرنسي أنه من المتصور أن يقع الاحتيال على نظام الحاسب وما يحويه من بيانات ومعلومات، ومن ثم إيقاعه في الغلط بقصد سلب الأموال، على اعتبار أن هذا الفعل تتوافر فيه الطرق

(1) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 124.

(2) د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1979، ص 892.

(3) Indira Carr & Katherine S Williams، Securing The E،Commerce Environment Enforcement Measures And Penalty Levels In The Computer Misuse Legislation Of Britain, Malaysia And Singapore، Computer Law & Security Report Vol. 16 No. 5 2000 P 295.

وفي واقعة شهيرة أدان القضاء الإنجليزي متهمًا بجريمة الاحتيال كان يعمل في أحد البنوك في الكويت، وقام بتحويل أموال عن طريق الحاسوب من حسابات بعض الزبائن لحسابه الخاص في المملكة المتحدة، وتمت إدانته بتهمة الحصول على أموال بطريق الخداع.

- محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، مرجع سابق، ص 183.

الاحتيالية ككذب تدعمه الأعمال المادية أو الوقائع الخارجية، حيث تتوافر فيه بجانب الكذب واقعة خارجية متمثلة في إبراز أو تقديم المستندات أو المعلومات المدخلة إلى الحاسب، أو باستخدام مستندات غير صحيحة يخرجها الحاسب بناءً على ما وقع في برامجه أو في البيانات المخزنة داخله من تلاعب، كي يستولي من فعل ذلك على أموال لا حق له فيها.

ويستند هذا الاتجاه إلى حكم محكمة النقض الفرنسية بتطبيق عقوبة النصب على شخص وضع قطعًا معدنية بدل قطعة النقود في عداد أماكن الانتظار، وترتب على ذلك تشغيل الماكينة، واعتبرت المحكمة هذا الفعل من قبيل الطرق الاحتيالية، ويدعم هذا الاتجاه جانب من الفقه المصري، حيث يرى أن غش العدادات والأجهزة الحسابية نوع من تجسيد الكذب الذي تتحقق به الطرق الاحتيالية.[1]

والاتجاه الثالث: وتمثله الولايات المتحدة الأمريكية، حيث تطبق النصوص المتعلقة بالغش في مجال البنوك والبريد والتلغراف والاتفاق الإجرامي لغرض الغش على حالات النصب المعلوماتي.[2]

بل إن بعض القوانين المحلية في بعض الولايات الأمريكية[3] أصدرت قوانين في هذا الخصوص، وأضفت تعريفًا موسعًا للأموال بأنها: (كل شيء ينطوي على قيمة) ومن ثم يندرج تحت هذا التعريف الأموال المعنوية

(1) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 374.
(2) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 128.
(3) من تلك الولايات: أريزونا وكاليفورنيا وفلوريدا وجورجيا وميتشجان ومونتانا، كل منها أصدر قانونا لتعريف الأموال.

والبيانات المعالَجة، حيث تعاقب هذه القوانين على الاستخدام غير المسموح به للحاسب الآلي بغرض اقتراف أفعال الغش أو الاستيلاء على أموال.

وعلى المستوى الفيدرالي صدر قانون سنة 1984 يعاقب على "الولوج غير المشروع أو المصطنع في الحاسب الآلي" وتم النص فيه على عقاب كل من ولج عمدًا في حاسب آلي بدون إذن، أو كان مسموحًا له بالولوج فيه ولكنه استغل الفرصة التي سنحت له عن طريق هذا الولوج لأغراض لم يشملها الإذن، وقام عمدًا عن طريق هذه الوسيلة باستعمال أو تعديل أو إتلاف أو إفشاء معلومات مختزنة في الحاسب، متى كان هذا الأخير يعمل باسم ولصالح الحكومة الأمريكية، وطالما أثرت هذه الأفعال على أداء وظيفته.

ولهذا يرى الفقه إمكانية تطبيق هذا النص وبشروط محددة على النصب المعلوماتي، وهذه الشروط هي: الاستيلاء على مال الغير، واستخدام الحاسب الآلي، والتدخل مباشرة في المعطيات بإدخال معلومات وهمية أو بتعديل البرامج أو خلق برامج صورية، وعلاقة السببية، فيتعين أن يترتب على أفعال الاحتيال قيام الجاني بالاستيلاء على أموال الغير دون وجه حق، وذلك باستخدام الحاسب الآلي بوصفه أداة إيجابية في هذا الاستيلاء، وذلك أن الحاسب الآلي يعد أداة إيجابية في جريمة النصب المعلوماتي متى تم التدخل مباشرة في المعطيات بإدخال معلومات وهمية أو بتعديل البرامج أو خلق برامج صورية، وليس هناك صعوبة في اكتشاف الطرق الاحتيالية في هذه الحالات، وذلك كأثر الاستخدام التعسفي لبطاقات الائتمان الممغنطة متى استخدمت كأداة في جريمة النصب.[1].

ووفقا لقضاء محكمة النقض الفرنسية فإن التسليم في جريمة النصب

(1) د. جميل عبد الباقي، الإنترنت والقانون الجنائي، مرجع سابق، ص 92.

المعلوماتي يستوي أن يكون ماديًا أو ما يعادله.

ومن ناحية أخرى يلزم أن تتوافر علاقة السببية في جريمة النصب - بما فيها النصب المعلوماتي - ما بين فعل التدليس وبين النتيجة المتمثلة في تسليم المال[1].

وقد تتخذ جريمة النصب باعتبارها إحدى جرائم الاعتداء على مواقع التجارة الإلكترونية أحد الأشكال الآتية:

1) إعداد مزادات خادعة، حيث إن ما يتم عبر شبكة الإنترنت ليس ماديات يتم الاطلاع عليها واقتناؤها فورًا مثل المزاد التقليدي، وإنما مجرد صور لتلك المواد بما يزيد من فرص النصب، ويجعلها تعد الأكثر انتشارًا في العالم الافتراضي.

2) الاستيلاء على متعلقات الهوية مثل أرقام كروت الائتمان، وذلك بعرض مواقع خادعة يتم من خلالها الاستيلاء على هذه الأرقام، بأن يرتاد المجني عليه هذه المواقع بما يؤدي إلى وقوعه ضحية للاحتيال.

3) الاحتيال باستخدام أساليب الاستثمار، كالإعلان عن بيع أسهم شركات عبر شبكة الإنترنت، والقيام بتحويل قيمتها على أحد المصارف، وذلك بقصد الإعلان المزيف عن الوضع المالي للشركة بغرض رفع قيمة أسهمها والتأثير في سوق المال، ثم القيام ببيع هذه الأسهم بمجرد بروز الأثر الإيجابي للخديعة.

4) النصب بأسلوب انتحال الشخصية، فيقوم المجرم عن عمد بالحصول على منفعة اقتصادية كحيازة مال أو تحويله أو استخدامه بموجب

(1) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 547.

وثائق إثبات شخصية تخص آخرين.[1]

وعلى ذلك فإن النصب المعلوماتي إن كان محله الاستيلاء على النقود أو أي منقول مادي آخر له قيمة مادية فليس هناك مشكلة في تجريمه، كأن يتم التلاعب في البيانات المدخلة أو المخزنة بالحاسب أو برامجه بواسطة شخص يستخدم الحاسب باسمه أو باسم شركائه ليستخرج شيكات أو فواتير بمبالغ غير مستحقة يستولي عليها الجاني أو يتقاسمها مع شركائه.

وإذا كان محل التسليم غير مادي وتحديدًا في حالة النصب المعلوماتي فإن جانبًا من الفقه الفرنسي يرى قيام الجريمة في حالة التدخل في البرمجة أو المعطيات المقدمة لجهاز الحاسب الآلي، والتي تؤدي إلى إلغاء رصيد مدين أو بالأحرى جعل الحساب دائنًا بمبالغ غير مستحقة؛ لأنه سواء قام الجاني باحتجاز أمر التحويل الخاص بشخص ما ثم زوره باسمه حتى يدفع قيمته في حسابه، أو تم التلاعب في البرنامج بهدف دفع الفوائد في حسابه فإن تحويل الأموال من حساب لآخر يتم بالقيد كتابة بدون تسليم الأموال للجاني، وفي كل هذه الفروض ورغم الطبيعة غير المادية للنقود الكتابية فإن الدفع يتم بواسطة القيد كتابة وهو ما يعادل التسليم المادي للأموال.

وجدير بالذكر أن المشرع الفرنسي قد نص في المادة (313-1) من قانون العقوبات الجديد على استخدام لفظ "النقود والأموال" كمحل لجريمة النصب، بعد أن تخلى عن لفظ "الأشياء" الوارد في المادة (405) من القانون القديم، أي لا يشترط في المال بالضرورة أن يكون من الأموال المادية.

كذلك تقوم جريمة النصب المعلوماتي وفقًا للنص الفرنسي- سالف الذكر متى كان محلها تقديم خدمة بناءً على النشاط الإجرامي الصادر من الجاني،

(1) د. عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، مرجع سابق، ص 417.

ولذلك فإن اختلاس الخدمات ليس سرقة حسب القانون الفرنسي، إنما هو استعمال طرق احتيالية للحصول على هذه الخدمة أي أنه يعد نصبًا.[1]

والنتيجة الحتمية لفعل الاحتيال هي أن يقوم المجني عليه بتسليم المال للجاني بمحض إرادته تحت تأثير الغلط، وهنا يثور تساؤل حول مدى اعتبار تسليم الحاسب الآلي ونظامه المعلوماتي المتصل بالشبكة المعلوماتية إنترنت المال إلى الجاني نتيجة فعل الاحتيال، وهل يعتبر ذلك من قبيل التسليم الذي تطلبه المشرع لإتمام الجريمة؟

لا تثور المشكلة إذا كان محل الجريمة في الاستيلاء الناشئ عن الاحتيال على الحاسب الآلي نقودًا أو أي منقول آخر له قيمة مادية، كأن يتلاعب الجاني في البيانات المدخلة أو المختزنة بالحاسب الآلي أو في برامجه، كي يستخرج الحاسب باسمه أو باسم شركائه شيكات أو فواتير بمبالغ غير مستحقة، ويستولي الجاني عليها أو يتقاسمها مع شركائه[2].

أما في حالة ما إن كان محل الاحتيال نقودًا كتابية أو بنكية، كأن يتم القيد الكتابي عن طريق التلاعب في البيانات المخزنة في الحاسب أو في برامجه لتحويل أموال الغير من حساباتهم إلى حسابه الخاص، فهنا تثور مشكلة مدى اعتبار ذلك من قبيل الاستيلاء المادي على المال من عدمه؟

ومعظم التشريعات لم تعتبر النقود الكتابية بمثابة مال عادي، بل توصفها بأنها من قبيل الديون والتي يستحيل أن تكون محلا للاختلاس أو السرقة، ومن أمثلة هذه الدول ألمانيا واليابان.

وعلى العكس من تلك التشريعات ذهبت بعض الدول إلى جواز اعتبار

---

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 144.

(2) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 282.

النقود الكتابية وعلى الرغم من طابعها غير المحسوس من قبيل الأموال التي تصلح لأن تكون محلا لجرائم السرقة والاحتيال، ومن أمثلة الدول التي أخذت بهذا الاتجاه كندا، وهولندا، وسويسرا، وإنجلترا، ومعظم الولايات المتحدة الأمريكية، حيث صدرت عدة قوانين أمريكية تعرف المال بأنه: (كل شيء يمثل قيمة، وهذا التعريف يشمل جميع الأموال الكتابية أو البنكية).[1]

وفي فرنسا صدرت بعض الأحكام من محكمة النقض الفرنسية تفيد أن الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم النقود[2].

وسميت هذه النظرية المبتدعة في القضاء الفرنسي بنظرية التسليم المعادل، وبناءً عليها فإن المادة (313) من قانون العقوبات الفرنسي الجديد تنطبق على جميع أفعال التلاعب في عملية البرمجة أو في البيانات المدخلة إلى الحاسب الآلي والمنقولة عبر شبكة الإنترنت، والتي قد تؤدي إلى إلغاء الرصيد المدين، أو خلق رصيد دائن بمبالغ غير مستحقة، وتتعدد الأساليب المستخدمة في هذا الشأن، فقد يحدث ذلك عن طريق التقاط أمر التحويل بواسطة الجاني وتزييفه بالأمر بتحويل نفس المبلغ لحسابه الخاص، أو عن طريق التلاعب في عملية البرمجة بغرض تحويل فوائد حساب شخص ما إلى حساب الفاعل، وأخيرًا عن طريق انتحال الفاعل لشخصية الغير ومباشرته لعملية تحويل النقود[3].

(1) محمد أمين الشوابكة، جرائم الحاسوب والانترنت، مرجع سابق، ص 1512.
(2) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص 283.
(3) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 134.

ويدعم هذا الاتجاه أيضًا بعض من الفقه المصري والذي يرى أن التسـليم في جريمـة النصـب يحققه وضع الشيء تحت تصرف الجاني، بحيث يتمكن من حيازته بغير عائق، ولو لم يستولِ عليه استيلاءً ماديًا[1].

ولما كانت جريمة النصب والاحتيال جريمة عمدية كما سبق البيان فإن صورة الركن المعنـوي فيها هو القصد الجنائي العام ثم القصد الخاص وهو نية التملك، وفي جريمـة النصـب المعلومـاتي يتحقق القصد العام إذا علم المتهم أنه يرتكـب فعـل تـدليس مـن شـأنه إيقـاع المجنـي عليـه في الغلط الذي يحمله على تسليم ماله، فالجاني يسـتخدم أسـلوبًا للإيهـام بوجـود ائـتمان كـاذب أو مشروع كاذب، ويتوصل إلى الاستيلاء على مال الغير كله أو بعضه متـى وقـع عـلى فـواتير الشراء باسم كاذب، أو استغل صفة كاذبة لتحويل أموال الغير من حساب إلى آخر عن طريـق التلاعـب في المعطيات أو البيانات المدخلة، ويجب توافر علمه بهذه الوقائع وأن تنصرف مـع ذلـك إرادتـه إليها رغم علمه بأن فعله من الأفعال التدليسية.[2]

أما عن القصد الجنائي الخاص وهو نيـة التملـك فيقـوم متـى كـان هـدف الجـاني مـن هـذا الاحتيال هو الاستيلاء على مال مملوك لغيره علمًا بأنه لا عبرة بالبواعث الدافعة لارتكاب جريمـة النصب، فيستوي أن يكون الباعث نبيلا أو غير ذلك.[3]

(1) راجع حول ذلك د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سـابق، ص 374، 375، ود. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا، مرجع سابق، ص 93 وما بعـدها (حول التسليم غير المتبوع بمناولة مادية)، ود. محمود نجيب حسني، شرح قانون العقوبات، ص 1036.

(2) د. أحمد حسام طه تمام، الحماية الجنائية للحاسب الآلي، دار النهضة العربية, 2000، ص 549.

(3) د.عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص595.

ويتوافر القصد الخاص في جريمة النصب المعلوماتي متى قام الجاني باستخدام البطاقة - مثلا - وهو عالم أن رصيده ليس به ما يكفي، أو أن بطاقته منتهية أو موقوفة ويستخدمها رغم ذلك في الحصول على سلع وخدمات، وكذلك قيام سارق البطاقة أو مزورها باستعمالها في الحصول على سلع أو خدمات مع علمه بأنه لا حق له في ذلك.[1]

الفرع الثاني

الحماية التي يسبغها تجريم النصب

على أموال التجارة الإلكترونية

بمطالعة النصوص التي تجرم النصب والاحتيال في قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة (المادة 399)، وفي القانون المصري (المادة 236)، وكذلك قانون العقوبات الفرنسي الجديد (المادة 313-1) نجد أنه لا فارق فيما بينها فيما يتعلق بالأموال العامة ولكن نص القانون الأخير (الفرنسي) أكثر قدرة على حماية الأموال في نطاق التجارة الإلكترونية من نص قانون العقوبات المصري والإماراتي.

هذا وقد عرف القانون الفرنسي النصب في المادة (313-1) بأنه (واقعة خداع شخص طبيعي أو معنوي، سواء باستعمال اسم كاذب أو صفة كاذبة، أو التعسف في صفة غير صحيحة، أو باستعمال حيلة تدليسية من شأنها حمل الغير على تسليم أموال أو قيمة أو مال ما، أو تقديم خدمة، أو الموافقة على عمل ينتج عنه التزام أو تحرر من التزام).

ولذلك لو قام أحد الأشخاص بطلب استشارة من طبيب أو محام عبر شبكة الإنترنت، وأوهمه بسداد أتعابه من خلال بطاقة الائتمان ولم يسددها،

(1) د. أحمد حسام طه، الحماية الجنائية للحاسب الآلي، مرجع سابق، ص 550.

فإنه يرتكب جريمة نصب حسب قانون العقوبات الفرنسي دون قانون العقوبات الإماراتي أو المصري، وذلك لأن قانون العقوبات الفرنسي يجعل الخدمات مساوية للمال الذي يمكن تسليمه في جريمة النصب، بمعنى أن الخدمات قد تكون موضوعًا للتسليم في جريمة النصب مثلها مثل المال تمامًا، ولذلك فإن المشرع الفرنسي في النص الجديد الذي يعاقب على جريمة النصب تحدث عن تسليم المال والخدمات وليس الأشياء، ولذلك فإن الفقه الفرنسي رأى في تخلي المشرع عن لفظ الأشياء أن التسليم قد يكون محله مالا معنويًا إلى جانب المال المادي.

وكذلك تقوم جريمة النصب - بحسب القانون الفرنسي - وعلى خلاف القانون المصري إن تمكن الجاني من الحصول على برنامج للكمبيوتر من شبكة الإنترنت أو سمع قطعة موسيقية أو اشترك في صحيفة عبر الشبكة، وذلك عن طريق وسائل احتيالية، ويعد المقابل في كل هذه الفروض عبارة عن المنفعة التي عادت عليه من الاستحواذ على البرنامج المعلوماتي أو سماع القطعة الموسيقية أو الاشتراك في الجريدة عبر شبكة الإنترنت، ولأن الانتفاع بالخدمة وتسليمها بناءً على طرق احتيالية في جريمة النصب يعادل سرقة المنافع في السرقة المعلوماتية؛ ذلك أن الأموال المعنوية أو الخدمات أو المنافع أو النقود الكتابية كلها نماذج لتطور المعلوماتية، والهدف من حمايتها حماية قيم أو كيانات ذات قيمة مالية، لكنها ليست نقودًا مادية يمكن قبضها باليد، غير أن لها ذات القيمة، ويمكن تحويلها إلى نقود مادية فيما بعد[1].

وقضى القضاء الفرنسي بدوره بأنه من الجائز استخدام نظم المعلومات في تحقيق جريمة النصب، ولذلك فقد قضي بأن "استخدام الكمبيوتر في

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 152.

اصطناع إيصالات وطبعها نظرًا لما له من إمكانيات في إجراء حسابات يمثل الإيهام بوجود دين غير حقيقي تقع به جريمة النصب"[1]، ويعقب الفقه الفرنسي على ذلك الحكم قائلا: إن الجاني لا ينصب على الآلة، ولكن ينصب على الإنسان الذي يجلس خلف هذه الآلة.

ومن ناحية أخرى تطبق أحكام جريمة النصب في القانون المصري وجريمة الاحتيال في قانون العقوبات الاتحادي لدولة الإمارات العربية المتحدة لو تمكن أحد من الحصول على مقابل مالي من المجني عليه والذي أوهمه - عن طريق شبكة الإنترنت - أنه طبيب معالج، ودعم ذلك باستخدام طرق احتيالية لتدعيم كذبه، ففي هذه الحالة يعاقب بجريمة النصب.

هذا بالنسبة لتطبيق القواعد العامة الواردة في قانون العقوبات على جرائم النصب المعلوماتي، ولكن في دولة الإمارات العربية المتحدة جاء القانون الاتحادي رقم 2006/2 في شأن مكافحة جرائم تقنية المعلومات بنص خاص يعاقب على ارتكاب جريمة النصب والاحتيال عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، حيث نصت المادة (10) منه على أن:

"كل من توصل عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات إلى الاستيلاء لنفسه أو لغيره على مال منقول أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية، أو باتخاذ اسم كاذب، أو انتحال صفة غير صحيحة، متى كان ذلك من شأنه خداع المجني عليه، يعاقب بالحبس مدة لا تقل عن سنة، وبالغرامة التي لا تقل عن ثلاثين ألف درهم، أو بإحدى هاتين العقوبتين".

(1) المرجع السابق، هامش ص 152.

والملاحظ على هذه المادة أنها تكرار للمادة الواردة في قانون العقوبات (399) إلا أنها حددت الوسيلة التي تتم من خلالها الجريمة وهي الشبكة المعلوماتية، أو إحدى وسائل تقنية المعلومات، كما نرى أن النص هنا سكت عند خداع المجني عليه ولم يستلزم تسليم الأموال للجاني؛ لأن ذلك يتماشى مع الاحتيال بالوسائل التكنولوجية الحديثة، فضلا عن أنه من المحتمل وقوع فعل الاحتيال على البرنامج أو وسيلة التقنية بحد ذاتها بالرغم من الخلاف الدائر بين الفقه - كما سبق وأن عرضنا - في مدى إمكانية ممارسة فعل الاحتيال على الحاسب الآلي وتعرضه للنصب والاحتيال، وبالتالي انطباق نص المادة سالفة الذكر على الواقعة.

كذلك أغفل النص سرقة المنفعة هنا أو الانتفاع بالخدمة التي يقدمها الموقع الإلكتروني، إلا إذا اعتبرنا مقابل هذه الخدمة مالا، وفي ذلك توسع في تفسير النص الجنائي القائم.

وأخيراً فإن الأموال المتداولة في نطاق التجارة الإلكترونية يمكن حمايتها بنصوص النصب والاحتيال، إلا أن الحماية في القانون الفرنسي ذات فاعلية أكثر من القانونين المصري والإماراتي بالرغم من النص الخاص الوارد في قانون مكافحة جرائم تقنية المعلومات، لأن القانون الفرنسي يراعي طبيعة المال المعلوماتي، خاصة وأن الشبكة المعلوماتية تتيح لنا الحصول على المنفعة والخدمات بقدر حصولنا على المنقولات والأشياء.

وبالاطلاع على نظام مكافحة جرائم المعلوماتية السعودي نجد أنه نص في المادة الرابعة على أن (يعاقب بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين؛ كل شخص يرتكب أيًا من الجرائم المعلوماتية الآتية :

1- الاستيلاء لنفسه أو لغيره على مال منقول أو على سند، أو توقيع هذا السند، وذلك عن طريق الاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة غير صحيحة.

كما نص القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها في المادة (10) بالقول: (كل من توصل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها إلى الاستيلاء لنفسه أو لغيره على مال منقول، أو على سند أو توقيع هذا السند، وذلك بالاستعانة بطريقة احتيالية، أو باتخاذ اسم كاذب، أو انتحال صفة غير صحيحة، متى كان ذلك من شأنه خداع المجني عليه يعاقب بالحبس....... وبالغرامة....... أو بإحدى هاتين العقوبتين".

الاتفاقية الأوروبية للجريمة الإلكترونية (بودابست 2001) نصت في مادتها الثامنة والمعنونة بجريمة النصب المتعلقة بالكمبيوتر، على أنه: (تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني إذا ما ارتكبت عمدًا وبغير حق، وتسببت في إلحاق خسارة بملكية شخص آخر عن طريق:

أ) أي إدخال أو تبديل أو محو أو تدمير لبيانات كمبيوتر.

ب) أي تدخل في وظيفة منظومة كمبيوتر بقصد احتيالي، أو غير آمن للحصول وبدون وجه حق على منفعة اقتصادية لصالح الشخص ذاته أو لصالح الغير.[1]

---

(1) د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية، مرجع سابق، ص 17.

والنص الإنجليزي للاتفاقية هو:

Article 8، Computer،related fraud

Each Party shall adopt such legislative and other measures as may be

ونصت مذكرة الاتفاقية التفسيرية على أنه ومع حدوث الثورة التكنولوجية The technological revolution تضاعفت إمكانيات ارتكاب جرائم اقتصادية كالغش Fraud، والنصب ببطاقات الائتمان Credit card fraud، كما أن الأصول الممثلة أو المتداولة عن طريق النظم المعلوماتية كالأموال الإلكترونية Electronic funds أو الودائع Deposit money أصبحت هدفًا للتلاعب بنفس الأشكال التقليدية للملكية.

وهذه الجرائم تتكون بشكل أساسي من خلال التلاعب بمدخلات النظام، بمعنى تغذية الحاسب ببيانات غير صحيحة، أو من خلال التلاعب في البرامج، أو من خلال تدخلات أخرى في معالجة البيانات.

والهدف المتوخى من هذه المادة تقرير الجزاء الجنائي المستحق لكل تلاعب تعسفي Any undue manipulation في سياق المعالجة الآلية للبيانات، ويكون من شأنه نقل غير شرعي للملكية An illegal transfer of property.

ومن باب الحرص على أن تكون كل أنواع التلاعب المتصورة قد أخذت في الاعتبار، فإن العناصر المكونة للإدخال Input، أو الإتلاف Alteration، أو المحو Deletion ، أو الطمس Suppression المبينة في الفقرة (أ) من المادة (8) يتم تكملتها بالإجراء العام للاعتداء على وظيفة الحاسب المنصوص عليها في الفقرة (ب) من المادة نفسها.

---

necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data,
b any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

ومما تجدر الإشارة إليه أن العناصر المكونة لمصطلحات الإدخال، والإتلاف، والمحو، والطمس، لها نفس المعنى الوارد في المواد السابقة.

كما أن الفقرة (ب) من المادة (8) تغطي أفعالا معينة، مثال ذلك التلاعب في المكونات المادية للحاسب، والأفعال التي تمنع المخرجات، والأفعال التي تؤثر على تسجيل أو تدفق البيانات، أو التسلسل الذي بمقتضاه يتم تحميل البرامج.(1)

يتوافر تجريم التلاعب الاحتيالي بالحاسوب إذا ترتب عليه خسارة اقتصادية مباشرة، أو حيازة لملكية الغير بشكل غير مشروع، وبشكل تتوافر فيه لدى مرتكب الجريمة نية تملك مكسب اقتصادي لنفسه أو لغيره، فمصطلح خسارة الملكية له مدلول موسع يتضمن خسارة النقود المادية وغير المادية ذات القيمة الاقتصادية.(2)

ويجب أن تكون الجريمة بدون حق، كما يجب أن يكون الحصول على المنفعة الاقتصادية دون حق أيضًا، وبالتالي فإن الممارسات التجارية العادية الشرعية، التي يتم تنفيذها بنية الحصول على منفعة اقتصادية، لا تعد جريمة في حكم هذه المادة، لأن الأفراد يتصرفون في نطاق حقهم القانوني، مثال ذ لك الأنشطة التي تتم بمقتضى عقد صحيح بين طرفين تكون مشروعة، ومثال ذلك النشاط الذي يكون محوره تعطيل موقع شبكة وفقًا لبنود العقد محل البحث.(3)

(1) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص 101.
(2) د. عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية، مرجع سابق، ص 89.
(3) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص 103.

ويشترط لتحقق القصد العام ارتكاب الجريمة عمدًا، ويشير القصد العام هنا إلى التلاعب بالحاسوب أو التداخل المسبب للخسارة في ملكية الغير، وتتطلب الجريمة أيضًا نية خاصة للاحتيال أو أية نية سيئة أخرى للحصول على مكسب اقتصادي أو غيره للنفس أو للغير، وعلى سبيل المثال فإن الأنشطة الاقتصادية التي تستند إلى المنافسة في السوق التي قد تتسبب في خسارة للفرد ومكسب لغيره، دون أن تكون مستندة إلى احتيال أو نية غير شريفة، لا تعد معنية في هذا الإطار الإجرامي بمقتضى هذه المادة[1]، ومثال آخر فإن استخدام برامج جمع المعلومات The use of information gathering programs من أجل المنافسة على شبكة الإنترنت، حتى لو كان غير مصرح به عند زيارة الموقع بواسطة صائد المعلومات Bot لا يعد معنيًا كذلك في هذا الإطار الإجرامي[2].



(1) د. عمر محمد بن يونس، الاتفاقية الأوروبية حول الجريمة الافتراضية، مرجع سابق، ص 90.

(2) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص 105.

الفصل الثاني

الجرائم الواقعة على البيانات

تمهيد وتقسيم:

ساهمت الطرق الإلكترونية السريعة لتبادل المعلومات في نمو وتطور العلاقات الاقتصادية والمعرفية بين المؤسسات والدول وبين الأفراد بعضهم البعض، وانعكس ذلك على نمو التجارة الإلكترونية عبر شبكة الإنترنت، والتي تمارس عن طريق الوسائل الإلكترونية، بما يعني تبادل البيانات إلكترونيًا واستخدام الوثائق الإلكترونية عن طريق مورد الخدمات الإلكترونية بطريقة تواصلية دون مراعاة للحدود الجغرافية ودون رقابة من أي من الدول[1].

كل ذلك أدى إلى إمكان أن تتعرض عمليات التجارة الإلكترونية فيما يتعلق بتداول البيانات لاعتداء تمثل في صورة جرائم حديثة لم تكن معروفة قبل ظهور هذه التجارة، والتقنيات المرتبطة بها من جهة، والمعلومات من جهة أخرى،، ومن أهم هذه الجرائم من وجهة نظرنا, والتي يتعين على أي مشرع أن يضعها في الاعتبار عند سن تشريع لحماية البيانات التعامل في البيانات بدون ترخيص، وانتهاك سرية وخصوصية البيانات، وجريمة التصريح عمدًا بمعطيات خاطئة، لذلك يتعين على المشرع عند وضع أي قانون لحماية المبادلات التجارية الإلكترونية أن يضع في الاعتبار مقتضيات حماية هذه التجارة من صور الاعتداء عليها، والتي تتمثل في التعامل في البيانات بدون ترخيص، وانتهاك سرية

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 36.

وخصوصـية البيانـات، والتصريـح عمـدًا بمعطيـات خاطئــة، والتلاعـب في بيانـات نظـم المعلومات، والاعتداء على نطاق أسماء الدومين.

وسوف نتناول كل واحدة في مبحث على حدة وفق الترتيب التالي:

المبحث الأول: جريمة التعامل في البيانات بدون ترخيص

المبحث الثاني: جريمة انتهاك سرية وخصوصية البيانـات

المبحث الثالث: جريمة التصريح عمدًا بمعطيات خاطئة

المبحث الرابع: جريمة التلاعب في بيانات نظم المعلومات

المبحث الخامس: الاعتداء على نطاق أسماء الدومين



المبحث الأول

جريمة التعامل في البيانات بدون ترخيص

يتسع مجال الحماية الجنائية للتجارة الإلكترونية ليشمل إلى جانب حماية مواقع التجارة الإلكترونية ووسائلها وأطرافها من موردين إلى تجار ومستهلكين، كافة الجرائم الواقعة على البيانات إذا كان بها مساس بالمصلحة المحمية؛ نظرًا لأن تداول البيانات المعلوماتية في أجهزة الحاسب الآلي وعبر شبكة الإنترنت بما فيها من بيانات التجارة الإلكترونية تقوم على أساس إجراء عمليات تجارية عن طريق وسيط إلكتروني، الأمر الذي يوجب الحصول مقدمًا على ترخيص بتداول هذه البيانات من الجهة المختصة، وفي دراسة جريمة التعامل في البيانات بدون ترخيص نتناول تعريف الجريمة وأركانها:

أولا: تعريف جريمة التعامل في البيانات بدون ترخيص:

تقوم التجارة الإلكترونية على أساس إجراء عمليات تجارية عن طريق وسيط إلكتروني، فكل ما يتعلق بالعملية التجارية من بيع أو شراء أو تفاوض أو عقود محلها بيانات معالَجة إلكترونيًا[1]، مما ساهم في نمو وتطور التجارة الدولية الإلكترونية في مختلف دول العالم نظرًا للطرق الإلكترونية السريعة لتبادل المعلومات عبر الشبكة الدولية، ونظرًا لأن هذه البيانات والمعلومات تنقل في شكل منتجات أو خدمات مما يكسبها قيمة مالية وتجارية فقد فرضت على المشرع الوطني والمشرع الدولي ضرورة فرض حماية جنائية، ليس بغرض منع الآخرين من الاستخدام المطلق للمعلومات، وإنما للحفاظ على سرية تداولها، إلا إذا كان هناك ترخيص بهذا

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص37.

التداول، لذلك يجب عند وضع أي تشريع لحماية التجارة الإلكترونية من صور الاعتداء عليها ضرورة النص على تجريم التعامل في البيانات بدون ترخيص، والترخيص تمنحه جهة مختصة يناط بها منح الترخيص بالتعامل في هذه البيانات دون غيرها من الجهات[1]، كما أن التعامل في هذه البيانات يجب أن يكون مقصورًا على أصحاب الشأن فيها وهم المتعاقدون، فلا يحق للغير التعامل فيها[2].

وقد نصت المادة 46 من القانون التونسي على أن: " يعاقب كل من يمارس نشاط مزود خدمات المصادقة الإلكترونية بدون الحصول على ترخيص مسبق... بالسجن لمدة تتراوح بين شهرين وثلاث سنوات، وبغرامة تتراوح من 1000 إلى 10.000 دينار، أو بإحدى هاتين العقوبتين".

وتعد هذه الجريمة من الجرائم المتكررة، ويتم الاعتداء بالتجسس غير المشروع على البيانات والمعلومات في مجال التجارة، ويشمل التجسس على الحسابات والموازنات وعناوين العملاء، والأسرار الصناعية والتجارية والمهنية، حيث تتوقف سرية البيانات في التجارة الإلكترونية على سهولة أو عدم سهولة اختراق نظامها للأمن والحماية، والتوفيق بين ذلك وبين حرية البيانات وإتاحتها وتداولها، ففي التجارة الإلكترونية يعني الدخول إلى هذه

(1) أوكل القانون الألماني الاتحادي الصادر سنة 1977 بشأن المعلوماتية الرقابة على تطبيق القانون إلى مفوض لنظم المعلومات يختص بحماية البيانات.
وفي فرنسا تختص اللجنة القومية للمعلوماتية والحريات المنشأة بموجب القانون رقم 78/ 17 في 1978/1/6 بإجراء الرقابة السابقة واللاحقة لحماية الحريات في مواجهة نظم المعلومات.
(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 22. .

المعلومات تمكين مجموعة من الأفراد دون غيرهم من الولوج إليها، بمعنى أن يكون متاحًا لشخص بعينه وبوصفه أحد المتعاقدين أو أحد المستهلكين الذين يهمهم أمر السلعة أو الخدمة المعلن عنها، فالخصوصية في نطاق التجارة الإلكترونية تعرف بأنها ارتباط هذه البيانات بالمتعاقدين من بائع لمشترٍ ومن منتج لمستهلك، والحقيقة أن سهولة التجسس والاختراق على الأسرار الصناعية والتجارية والمهنية من الأمور التي تعرقل التجارة الإلكترونية، بما يفرض ضرورة الحماية لتلك البيانات التجارية الإلكترونية، وعدم التعامل فيها بدون ترخيص.

وخلاصة القول أن جريمة التعامل في البيانات بدون ترخيص هي تلك الجريمة التي تقوم غالبًا من شخص اعتباري يمارس التعامل في بيانات التجارة الإلكترونية, وفي إصدار الشهادات الخاصة بالمصادقة الإلكترونية على التواقيع الإلكترونية, دون أن يكون حاصلا على ترخيص يخول له العمل بذلك من السلطات المختصة.

ثانيًا: الركن المادي لجريمة التعامل في البيانات بدون ترخيص:

يتمثل الركن المادي في هذه الجريمة في التعامل في بيانات التجارة الإلكترونية بدون ترخيص من الجهة المختصة، حيث تهتم الدول بضرورة وجود جهة تختص بإصدار الترخيص أو الإذن في التعامل في البيانات المعلوماتية، وقد اهتمت معظم الدول الأوروبية بإنشاء أجهزة رقابة وإشراف، أما الدول التي لم تأخذ بإنشاء هذه الأجهزة فإنها تأخذ بالإشراف القضائي اللاحق في حالة حصول مخالفة من المخالفات، وفي البلاد العربية توجد بعض الجهات لإصدار هذه التراخيص منها شبكة المعلومات للعلوم والتكنولوجيا بأكاديمية البحث العلمي والتكنولوجيا في مصر، وغيرها من الجهات في الإمارات والسعودية والكويت.

لم يورد القانون الإماراتي رقم 1 /2006 في شأن المعـاملات والتجـارة الإلكترونيـة أيـة نصـوص بخصوص التعامل في البيانـات بـدون تـرخيص مسـبق، بـالرغم مـن نصـه عـلى الأحكـام المتصـلة بشهادات المصادقة الإلكترونية، وخـدمات التصـديق، حيـث نـص في المـادة (20) منـه عـلى أنـه: (لأغراض هذا القانون يعين بقرار من مجلس الوزراء جهة لمراقبة خدمات التصديق، وعـلى وجـه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي خدمات التصديق والإشراف عليها).

إلا أن القانون الإماراتي حاول تنظيم بعض الأمور الخاصة بشهادات المصادقة وإسباغ حمايـة جنائية عليها، فنص في المادة (28) منه على أنه: (لا يجوز لأي شـخص أن ينشر شـهادة تشـير إلى مزود خدمات تصديق مدرج اسمه في الشهادة، إذا كان الشخص يعرف أن:

أ) مزود خدمات التصديق المدرج اسمه في هذه الشهادة لم يصدرها.

ب) الموقع المدرج اسمه في الشهادة لم يقبلها.

ج) هذه الشهادة قد ألغيت أو أوقفت، إلا إذا كان ذلـك النشر بغـرض التحقـق مـن توقيـع إلكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء).

وهنا القانون أتى بثلاث صور متوقعة الحدوث، الأولى أن يقوم أحدهم بنشر شهادة تصـديق إلكتروني مدعى صدورها إلى مزود خدمات تصديق معين، دون ذكر اسمه في الشـهادة في الوقـت الذي لم تصدر عنـه هـذه الشـهادة، والثانيـة تخلـص في قيـام أحـد الأشـخاص باسـتعمال شـهادة تصديق إلكتروني تم رفضها من قبل الموقع لأي سبب كان، والصـورة الثالثـة تتمثـل في أن الجـاني يستعمل شهادة تصديق ملغاة أو موقوفة بصفة مؤقتة، إلا إذا كان الاسـتعمال هدفـه الاسـتيثاق من توقيع إلكتروني أو رقمي تم استعماله قبل

صدور قرار الوقف أو الإلغاء.[1]

كما أن القانون الإماراتي أتى بجريمة مقاربة للجريمة التي نحن بصددها حينما نص في المادة (26) منه على أن: (يعاقب بالحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن خمسين ألف درهم ولا تزيد على مائتين وخمسين ألف درهم، أو بإحدى هاتين العقوبتين كل من أنشأ أو نشر أو وفر أو قدم أية شهادة مصادقة إلكترونية تتضمن أو تشير إلى بيانات غير صحيحة مع علمه بذلك).

والملاحظ أن النص السابق أسبغ الحماية الجنائية على شهادة المصادقة الإلكترونية، وهي تلك الشهادة التي يصدرها مزود خدمات التصديق يفيد فيها تأكيد هوية الشخص أو الجهة الحائزة على أداة توقيع معينة[2]، فالقانون جرم من يضمن هذه الشهادة أية معلومات غير صحيحة، سواء أكان منشأ هذه الشهادة الجهة المخولة قانونًا بإصدارها، أو من قام بنشرها أو توفيرها أو تقديمها للغير، واشترط علم الجاني بعدم صحة البيانات الواردة في شهادة المصادقة الإلكترونية.

والركن المادي في هذه الجريمة يقوم على إنشاء أو نشر أو توفير شهادة بيانات غير صحيحة، ويتحقق الإنشاء عن طريق اختلاق الشهادة التي ليس لها وجود، أي اصطناعها، وكذلك اصطناع بيانات غير صحيحة، ثم نشر هذه الشهادة أو البيانات غير الصحيحة واستعمالها من قبل الجاني الذي قام

(1)د. خالد محمد المهيرى، النظام القانوني للتجارة الاليكترونية في دولة الإمارات العربية المتحدة، ط. ثانية، معهد القانون الدولي، دبي، 2004، ص 447 وما بعدها.

(2) المادة (1) والخاصة بالتعاريف في قانون المعاملات والتجارة الإلكترونية الإماراتي 1 / 2006.

بالإنشاء أو النشر مع علمه بذلك.

ولابد أن ينصب فعل الإنشاء أو النشر على مستند إلكتروني معين هو شهادة التصديق الإلكتروني التي تصدر عن مزودي خدمات التصديق الإلكتروني.

والمقصود بالبيانات هي أية معلومات تتعلق بالمعاملات الإلكترونية التي تستخدم فيها شهادة التصديق حتى ولو تعلقت بطرفي العقد، ويشترط في الشهادة أو البيانات أن تكون غير صحيحة، وهذه الجريمة تقع على بيانات التجارة الإلكترونية، ومن شأن وقوعها التأثير سلبًا على نمو وازدهار هذه التجارة[1].

وقد جاء النص الوارد في القانون المحلي لإمارة دبي أكثر انفتاحًا في مجال التجريم عندما نص في المادة (1/39) منه على أن: (يعاقب كل من أنشأ أو نشر عن معرفة، أو وفر أية شهادة أو بيانات غير صحيحة لأي غرض احتيالي أو أي غرض آخر غير مشروع بالحبس، وبغرامة لا تجاوز 250.000 درهم، أو بإحدى هاتين العقوبتين).

كما ينتقد أيضًا مشروع قانون التجارة الإلكترونية المصري لأنه لم يهتم بتجريم التعامل في البيانات بدون ترخيص، ولم يرد في الفصل العاشر منه والمخصص للجرائم والعقوبات أي نص يشير لأي تجريم في التعامل في البيانات المعالجة إلكترونيًا بدون ترخيص، وكان يجب على هذا المشروع النص على تجريم هذه الصورة، وهذا النقص من مبررات النقد

---

(1) د. خالد محمد المهيري، النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة، مرجع سابق، ص 459.

- ولقد نص على هذه الجريمة في المادة (28) من مشروع قانون التجارة الإلكترونية المصري.

الذي يوجه لهذا المشروع الذي تؤخذ عليه العديد من الانتقادات خاصة في الصياغة، بل إن المشروع لم يذكر البيانات إلا عرضًا وفي أثناء التعرض لموضوع يختلف تمامًا عن تناولها، ففي الفصل الرابع منه والمخصص لموضوع التشفير الإلكتروني نوه المشروع عن ضرورة حماية البيانات المشفرة، وقصر فضها على صدور أمر قضائي[1].

إلا أن قانون التوقيع الإلكتروني المصري رقم (15) لسنة 2004 نص في المادة (23)[2] على جريمة إصدار شهادة تصديق إلكتروني دون الحصول على ترخيص مزاولة النشاط من الهيئة، فهذا النص عالج حالة واحدة من حالات التعامل في البيانات بدون ترخيص وهي حالة إصدار شهادة التصديق الإلكتروني فقط.

أما التشريع التونسي فقد كان موقفه مختلفًا عن مشروع القانون المصري المشار إليه، فقد اهتم المشرع التونسي بمعالجة موضوع التجارة الإلكترونية معالجة تفصيلية غطى بها كافة جوانب الموضوع، ومن ضمنها اهتمامه بتجريم الاعتداء على تداول البيانات الإلكترونية بدون ترخيص وذلك في نص المادة (46) منه السابق بيانها, والتي تعاقب على ممارسة نشاط مورد المصادقات والوثائق الإلكترونية بدون الحصول على

(1) راجع نص مشروع قانون التجارة الإلكترونية المصري، الفصل الرابع والفصل العاشر.
(2) المادة (23) من قانون التوقيع الإلكتروني المصري تنص على أنه:
"مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من:
(أ) أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة..."

ترخيص مسبق.

كما نصت المادة (44) من القانون ذاته على سحب الترخيص من مورد الخدمات الإلكترونية وإيقاف نشاطه إذا أخل بواجباته[1].

يضاف إلى ذلك نص المادة (45) من القانون التي تعاقب على عدم مراعاة قواعد كراسة الشروط من جانب مورد الخدمات الإلكترونية[2].

والركن المادي لهذه الجريمة كما أشرنا يتوافر بمجرد تداول البيانات بدون ترخيص مسبق ولو لم يترتب على ذلك أي ضرر، فالجريمة تعتبر من جرائم الخطر أو جرائم السلوك المجرد، فلا تتطلب تحقيق نتيجة معينة[3].

ولم يهتم القانون الأردني الخاص بالمعاملات الإلكترونية بهذه الجريمة أيضًا، وإنما سار على نفس ما سار عليه المشرع الإماراتي في تجريمه إنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالي أو لأي غرض غير

(1) نصت المادة 44 من القانون التونسي على أن: " يسحب الترخيص من مزود خدمات المصادقة الإلكترونية ويتم إيقاف نشاطه، إذا اخل بواجباته المنصوص عليها بهذا القانون أو بنصوصه التطبيقية. وتتولى الوكالة الوطنية للمصادقة الإلكترونية سحب الترخيص بعد سماع المزود المعني بالأمر ".

(2) نصت المادة 45 من القانون التونسي على أنه: " علاوة على العقوبات المبينة بالفصل 44 من هذا القانون، يعاقب كل مزود خدمات المصادقة الإلكترونية لم يراع مقتضيات كراس الشروط المنصوص عليه بالفصل 12 من هذا القانون بخطية تتراوح بين 1.000 و10.000 دينار. "

(3) د. عبد الأحد جمال الدين، النظرية العامة للجريمة، دار الثقافة الجامعية، القاهرة، 1993، ص 311، وفي هذا المعنى: د.عوض محمد عوض، قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية، 1991، ص 64، د. يسر أنور علي، شرح قانون العقوبات، القاهرة، 1993، ص 251.

مشروع[1].

ثالثًا: الركن المعنوي لجريمة التعامل في البيانات بدون ترخيص:

جريمة التعامل في البيانات بدون ترخيص هي جريمة تقع بطريق العمد وطريق الخطأ غير العمدي؛ لأن الشخص قد يخطئ في تداول تلك البيانات بدون حصوله على الترخيص اللازم، وبذلك يكون قد خالف اللوائح والقوانين في صورة الخطأ غير العمدي، ولكن قد يتعمد تداولها بدون ترخيص وهو على علم بذلك، ويتمثل العمد وهو القصد الجنائي في انصراف إرادة الجاني إلى تداول بيانات التجارة الإلكترونية بدون ترخيص، مع علمه بأن ذلك محظور ومعاقب عليه بموجب القانون، ويكتفى في هذه الجريمة بالقصد الجنائي العام.

والقانون التونسي نص على عقاب رادع لهذه الجريمة بالمادة (46) من قانون التجارة الإلكترونية، وهو عقوبة السجن مدة تتراوح بين شهرين و3 سنوات، وغرامة من 1000 الى10.000 دينار أو أحدهما.

يضاف إلى ذلك أن نص المادة (45) قد عاقب على عدم مراعاة قواعد كراسة الشروط المنصوص عليها بالقانون بالغرامة من 1000 إلى 10.000 دينار، ثم لم يكتف القانون بذلك، بل نص في المادة (44) منه على سحب الترخيص من مورد خدمات الوثائق الإلكترونية وإيقاف نشاطه إذا أخل بواجباته التي نص عليها هذا القانون.

(1) جاء نص المادة (35) من قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001 على أن: (يعاقب كل من يقوم بإنشاء أو نشر أو تقديم شهادة توثيق لغرض احتيالي، أو لأي غرض غير مشروع، بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين، أو بغرامة لا تقل عن (3000) ثلاثة آلاف دينار، ولا تزيد على (10.000) عشرة آلاف دينار، أو بكلتا هاتين العقوبتين).

وأخيراً فإننا نرى أن التعامل في بيانات التجارة الإلكترونية بدون ترخيص من جانب مزود الخدمات الإلكترونية أمر يستلزم من التشريعات إلزامه بالتزامات محددة وإلا خضع لعقاب حاسم، وذلك لما تمثله هذه البيانات من أهمية لصاحبها أو للغير المعني بها، وعدم السماح لكل من شاء بالتعامل في هذه البيانات، وإنما يجب أن يكون هذا التعامل تحت مظلة القانون.



المبحث الثاني

جريمة انتهاك سرية وخصوصية البيانـات

تتناول هذه الجريمة انتهاك سرية وخصوصية البيانات باعتبار أن البيانات المتعلقة بالتجـارة الإلكترونية محصورة في نطاق عدد محدود من الأشخاص، ولا يمكن تصور جريمة انتهاك البيانـات إذا انعدم هذا الحصر نظرًا لأن المعلومة غير السرية قابلة للتداول وتكون بمنـأى عـن أيـة حيـازة خاصـة، وسريـة المعلومـات قـد تكـون بـالنظر إلى طبيعتهـا، أو إلى إرادة صـاحبها أو حائزهـا، أو بالأمرين معًا كرقم بطاقة الائتمان الكودي التي لا يمكن التعامل بها إلا عـن طريـق هـذا الـرقم، وعلى ذلك فإن البيانات رغم كونها غير مادية إلا أن لها دلالات مادية فهي تصلح لأن تكون محلا لحق الملكية، ومن ثم وجب أن تتمتع بحماية القانون الجنائي سواء أكانـت المعلومـة سياسـية أو اقتصادية أو علمية، وسنبدأ بتعريف الجريمة، ثم بيان ركنها المادي، ثم المعنوي، وذلك في النقـاط الآتية:

أولا: تعريف الجريمة:

لا يوجد نص في القانون يعطي تعريفًا جامعًا مانعًا للمعلومة، والقانون الفرنسيـ الصـادر في 1982/7/29 الخاص بالاتصالات السمعية والبصرية أشار إلى أول تعريف للمعلومة بأنهـا: " رنـين صور الوثائق والبيانات أو الرسائل من أي نوع "، وعرفها الفقه الفرنسي بأنها: "رسالة معـبر عنهـا في شكل يجعلها قابلة للنقل أو الإبلاغ للغير"، ويعرفهـا آخـرون بأنهـا: " رمـز أو مجموعـة رمـوز تنطوي على إمكانية الإفضاء إلى معنى محدد"[1]، ويقصد

(1) Christinae Feral.Schuhl، CYBER DROIT، Le droit a' l'e'preuve de l'internet op cit- p 219.

بالبيانات أو المعلومات في هذه الجريمة تلك البيانات المعالجة إلكترونيًا[1].

وتعرف هذه البيانات بأنها تلك التي يتم التعامل بها في نطاق التجارة الإلكترونية، وهي شيء غير مادي، ولكنها تصلح لأن تكون محلا للحقوق المالية، فقد تمثل المعلومة منتجًا أو سلعة أو خدمة، فيجب الحفاظ على سريتها وخصوصيتها تأمينًا لممارسة العملية التجارية، بمعنى التعامل مع المعلومة على أنها حقيقة في ذاتها، ويتم التعامل معها بالنظر إلى قيمتها الثقافية والسياسة والاقتصادية، وهو ما يرفع المعلومة إلى مصاف الأموال، فتصبح المعلومة محلا للتعامل، ويتحدد سعرها وفقًا لظروف العرض والطلب، ويلقى العبء على نظام الأمن لحماية البيانات وتأمين سريتها.

وتختلف أنظمة الأمان في مدى السرية التي توفرها للبيانات من حيث سهولة أو عدم سهولة اختراق النظام، حيث إن حماية نظام المعلومات يعتمد على عدة عوامل أهمها السرية، وحرية تداول البيانات وإتاحتها Availability، ثم سلامة البيانات، والسرية تعني عدم معرفة الغير من غير المتعاقدين ببيانات العملية التجارية، والخصوصية تعني ارتباط هذه البيانات بالمتعاقدين أطراف العملية التجارية مما يحتم عدم اطلاع الغير عليها[2].

ولا يمكن أن نكون بصدد بيانات معالجة إلكترونيًا عن التجارة

---

(1) د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية للتجارة الإلكترونية، مرجع سابق، ص 279.

(2) Keith Harrison, Bill Munro and Tim Spiller, HP Laboratories، Security through uncertainty، Network Security Magazine، February 2007، p p 4,5.

الإلكترونية ما لم يكن لدينا نظام معلوماتي يتقبل بيانات هذه التجارة كمدخلات ثم يتولى تشغيلها وتحليلها وإخراجها إلينا في صورة مخرجات وهي البيانات الإلكترونية المتعلقة بالتجارة الإلكترونية والتي هي موضوع الحماية الجنائية في الجريمة التي نحن بصدد دراستها[1].

نصت المادة (52) من القانون التونسي الخاص بالتجارة الإلكترونية على أنه: (يعاقب طبقًا لأحكام الفصل 254 من المجلة الجنائية مزود خدمات المصادقة الإلكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم، باستثناء تلك التي رخص صاحب الشأن كتابيًا أو إلكترونيًا في نشرها أو الإعلام بها، أو في الحالات المنصوص عليها في التشريع الجاري العمل به).

ويمكننا القول بأن جريمة انتهاك سرية وخصوصية البيانات هي تلك الجريمة الماسة ببيانات ومعلومات خاصة بصاحبها ولا يرغب في نشرها أو إطلاع الغير عليها, وأن يقوم الجاني الذي عهد إليه بهذه البيانات والمعلومات واطلع عليها بحكم عمله, بنشرها خلافا لإرادة صاحبها.

ثانيًا: الركن المادي لجريمة انتهاك سرية وخصوصية البيانات:

تتحقق خصوصية البيانات وسريتها في التجارة الإلكترونية عبر وسائل فنية وتقنية، بحيث تحجب هذه المعلومات عن أي شخص ليس له حق الاستفادة منها، بمعنى أن هذه البيانات ترتبط بالمتعاقدين في التجارة الإلكترونية كالبائع والمشتري أو المنتج والمستهلك.

ويتحقق الركن المادي للجريمة بمجرد انتهاك سرية البيانات وخصوصيتها حتى ولو لم يترتب على الفعل أي نتيجة، فالجريمة سلوكية

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 41.

يكتفي المشرع فيها بتحقيق السلوك الإجرامي بدون اشتراط تحقق نتيجة؛ لأن الغرض من التجريم هو الحفاظ على سرية وخصوصية البيانات وليس منع تحقق نتيجة إجرامية[1].

وتطبيقًا لذلك فإننا نجد أن مشروع قانون التجارة الإلكترونية المصري اهتم بموضوع سرية البيانات المشفرة واحترام الحق في الخصوصية، وجرم الفعل الصادر بانتهاك السرية والخصوصية من أي شخص سواء بالذات أو بالوساطة، بكشف مفاتيح التشفير المودعة بمكتب كشف الشفرات أو إساءة استخدامه بأي صورة من الصور، وكذلك عاقب كل من يقوم بفض معلومات مشفرة في غير الأحوال المصرح بها قانونًا، وقد ورد النص عامًا بحيث يجرم انتهاك السرية والخصوصية الصادر من أي شخص بالذات أو الوساطة، وسواء كان مورد الخدمات أو غيره، وإن كان قيد السرية والخصوصية من الالتزامات الواقعة على مورد الخدمات في مواجهة أطراف التعاقد.

في حين أن القانون التونسي في المادة (52), السابق بيانها, كان أكثر تحديدًا بنصه على تجريم الاعتداء على السرية والخصوصية بإفشاء معلومات عهدت إلى مورد الخدمات الإلكترونية في إطار نشاطه، باستثناء تلك التي رخص له صاحب الشأن بمقتضى شهادة كتابية أو إلكترونية بنشرها.

ثالثًا: الركن المعنوي للجريمة:

جريمة انتهاك سرية البيانات وخصوصيتها هي من الجرائم العمدية، ويتمثل الركن المعنوي لتلك الجريمة في القصد الجنائي العام بعنصريه العلم

(1) د. عوض محمد عوض، قانون العقوبات، القسم العام، مرجع سابق، ص 55.

- Directive European N 2000،31، du 8 jun 2000،.art. 6.

والإدارة، فالجاني هنا يسعى بإرادته إلى فض مفاتيح تشفير المعلومات في غير الأحوال المصرح بها قانونًا، وذلك مع علمه التام بماديات الواقعة المؤثمة قانونًا، وأنه على علم بمكونات الواقعة المتمثلة في فض شفرة المعلومات، وقبوله النتيجة المترتبة عليها.

وذهب رأي إلى إمكانية تصور ارتكاب الجريمة عن طريق الخطأ إذا قام الجاني بفض الشفرة في حالة غير تلك الحالات المصرح بها قانونًا، ذلك أن المبدأ الذي وضعه المشرع في مشروع قانون التجارة الالكترونية المصري هو تجريم فعل فض الشفرة بالذات أو الوساطة بأي صورة من الصور في البداية، ثم أعقب ذلك في حالة أخرى بقوله: (وكذلك على من يقوم بفض معلومات مشفرة في غير الأحوال المصرح بها قانونًا)[1].

والقانون التونسي في المادة (52) منه قد عاقب مزود أو مورد الخدمات الإلكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم، وهو بذلك يشترط توافر القصد الجنائي كجوهر للركن المعنوي لجريمة الإفشاء.

رابعًا: جريمة إفشاء الأسرار الإلكترونية في قانون المعاملات والتجارة الإلكترونية الإماراتي:

تجرم المادة (28) من القانون الاتحادي الإماراتي إفشاء الأسرار الإلكترونية حيث نصت على أنه:

1) يعاقب بالحبس مدة لا تقل عن ستة أشهر، والغرامة التي لا تقل عن عشرين ألف درهم ولا تزيد على مائتين ألف درهم، أو بإحدى هاتين

(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 43، ويراجع نصوص الفصل العاشر من مشروع التجارة الإلكترونية المصري بعنوان الجرائم والعقوبات، المبدأ الأول، ص 8.

العقوبتين كل شخص تمكن بموجب أية سلطات ممنوحة لـه في هـذا القـانون مـن الاطـلاع عـلى معلومات في سجلات أو مستندات أو مراسلات إلكترونية وأفشى أيًا من هذه المعلومات.

2) يستثنى من أحكام الفقرة (1) من هـذه المـادة حـالات التصريح بالمعلومـات التـي تـتم لأغراض تنفيذ هذا القانون، أو تنفيذًا لأية إجراءات قضائية.

ووفقا لهذا النص فإنه يجرم الحالة التي يقوم فيها أي شخص استطاع لسبب منصوص عليـه في هـذا القـانون أن يطلـع عـلى معلومـات مدونــة في السـجلات أو المراسـلات أو المسـتندات الإلكترونية، ثم يقوم بإفشائها متعمدا أو تسبب بإهماله في إفشاء هذه المعلومات[1].

ويمكن القول بأن صورة السلوك الإجرامي ضمن الركن المادي في هذه الجريمـة تخلـص في أن الجاني وفي نطاق التجـارة الإلكترونيـة قـد اطلـع عـلى المعلومـات أو السـجلات أو المسـتندات أو المراسلات الإلكترونية، ثم قام عامدًا بإفشـاء سر هـذه المعلومـات أو البيانـات، أو أفشى بطريـق الإهمال، على أن يكون ذلك بوسيلة إلكترونية بما فيها تقنيات الاتصالات الحديثة.

ويشترط كذلك أن تؤدي عملية الإفشاء إلى هتك طابع السرية الذي تتسم به استنادًا لكونها تتعلق بعقد إلكتروني أو صفقة إلكترونية، ومن مصلحة الأطراف عدم إفشـائها، ويسـتوي أن يـتم الإفشاء بمقابل أو بدون مقابل، لكن المعول عليه أن تؤدي عملية الإفشاء إلى فقـد طـابع السريـة الذي تتسم به.

والذي يحدث في هذه الجريمة أن الجاني يطلع عـلى معلومـات إلكترونيـة، ويقصـد بهـا أيـة معلومات مدونة في شكل سجل إلكتروني أو مستند إلكتروني

(1) د. عبد الفتاح بيومي حجازي، مقدمة التجارة الإلكترونية العربية، مرجع سابق، ص275.

أو رسالة إلكترونية، وأن يكون اطلاع الشخص على هذه المعلومات الإلكترونية مبررًا، كأن يكون من مزودي خدمات شبكة الإنترنت المنوط بهم توصيل هذه الخدمة إلى العملاء، وقد يكون من مزودي خدمات التصديق الذين يصدرون شهادة التصديق على التوقيع الإلكتروني أو صحة بيانات المتعاقد في نطاق التجارة الإلكترونية، وقد يكون من الأشخاص العاملين لدى مراقب خدمات التصديق الذي يتولى هو ومعاونوه التفتيش على مزودي خدمات التصديق ومدى التزامهم بأحكام القانون، مؤدى ذلك أن الجاني يكون له دائمًا حق الاطلاع على المعلومات الإلكترونية التي تم الاطلاع عليها[1].

وهذه الجريمة من الجرائم القصدية التي تقوم على القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني بحقيقة أفعاله وأن المشرع يؤثمها، وهو فعل الإفشاء، ومع ذلك تنصرف إرادته إلى ذلك الفعل، ويقبل كافة النتائج المترتبة على ذلك الفعل من انتهاك سرية البيانات الإلكترونية والإضرار بأصحابها.

وقد أتى النص بسبب إباحة يتمثل في أن الجاني قد يفشي سرًّا من الأسرار الإلكترونية التي اطلع عليها أو اؤتمن عليها، وكان سبب الإفشاء يرجع إلى تصريح بنص القانون أو التنفيذ استنادًا لإجراءات قضائية، كأمر يصدر من إحدى المحاكم المختصة.

ففي الفروض السابقة يتمتع الشخص بسبب إباحة مصدره نص القانون نفسه، حيث تحول فعل الإفشاء محل التجريم في الجريمة التي نحن بصددها إلى فعل مباح، وبالتالي لا يعاقب مَن أتاه[2].

(1) المرجع السابق، ص 276.
(2) د. خالد محمد المهيري، النظام القانوني للتجارة الإلكترونية في دولة الإمارات =

وهذه الجريمة تقترب من جريمة انتهاك السرية والخصوصية في التجارة الإلكترونية، والتي تتحقق عن طريق اختراق نظم البيانات الخاصة بها والاستيلاء عليها أو محاولة تدميرها أو إتلافها، لكن الفارق بينهما أن الجريمة الأخيرة تقع من شخص غير مصرح له قانونًا بالاطلاع على هذه البيانات، لذلك يلجأ إلى الاختراق.

وقد نص القانون المحلي لإمارة دبي على الجريمة نفسها، ولكن نص صراحة على صورة التسبب بالإهمال في إفشاء هذه المعلومات، حيث جاء النص عليها في الفقرة الثانية من البند (1) من المادة (31) على النحو التالي: (وتكون العقوبة الغرامة التي لا تجاوز (100.000) درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات).[1]

ونص المشرع التونسي على حالة لم يتناولها المشرع الإماراتي، وهي حالة الترخيص بنشر البيانات بمقتضى شهادة كتابية أو إلكترونية من صاحب الشأن، فكان أكثر تحديدًا، وهي حالة واردة في مجال التجارة

= العربية المتحدة، مرجع سابق، ص 473 وما بعدها.

(1) نصت المادة (31) من قانون إمارة دبي رقم 2 لسنة 2002 في شأن المعاملات والتجارة الإلكترونية على أنه:
1- يعاقب كل شخص تمكن بموجب أية سلطات ممنوحة له في هذا القانون من الاطلاع على معلومات في سجلات أو مستندات أو مراسلات إلكترونية، وأفشى متعمدًا أيًا من هذه المعلومات بالحبس، وبغرامة لا تجاوز 100.000 درهم، أو بإحدى هاتين العقوبتين، وتكون العقوبة الغرامة التي لا تجاوز 100.000 درهم في حالة تسببه بإهماله في إفشاء هذه المعلومات.
2- يستثنى من أحكام الفقرة (1) من هذه المادة حالات التصريح التي تتم لأغراض هذا القانون، أو أية إجراءات جزائية حول جرم ارتكب بالمخالفة لأي قانون، أو لأغراض الأوامر الصادرة عن أية سلطة قضائية.

الإلكترونية ففي أحيان كثيرة يتم نشر بيانات خاصة بموافقة صاحبها، وبالتالي لا تقوم الجريمة حينها.

وهذه المسألة تناولها القانون التونسي في المادة (52) من قانون التجارة الإلكترونية التونسي، وأغفل المشرع الإماراتي النص عليها في القانون الحالي رقم 1 لسنة 2006 في شأن التجارة والمعاملات الإلكترونية، كما أغفل النص عليها في قانون إمارة دبي رقم 2 لسنة 2002 في شأن التجارة والمعاملات الإلكترونية، ولذلك فإنه لا مناص عند تجريم هذا الفعل حال وقوعه من الرجوع إلى القواعد العامة في قانون العقوبات الاتحادي رقم 3 لسنة 1987[1].

يذكر أن المشرع الإماراتي في هذا النص أغفل أيضًا حالة العقاب على إفشاء هذه الأسرار بطريق الإهمال، وما كان يجب أن يسقط المشرع في ذلك، لاسيما وأن قانون إمارة دبي المحلي رقم 2 لسنة 2002 في شأن التجارة الإلكترونية قد عالج هذه المسألة وعاقب عليها في نص الفقرة الثانية من المادة (31) من القانون المذكور، والتي تتحقق صورتها بأن يهمل الجاني أو لا يحتاط في الحفاظ على الأسرار الموكولة له، فتسقط الأسرار أو المعلومات في يد غيره فيسرق الأقراص والأسطوانات المدمجة المدون عليها هذه المعلومات، وذلك بسبب عدم احترازه، وقد عاقب المشرع في قانون إمارة دبي على هذه الجريمة بالغرامة فقط[2].



(1) د. عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الإلكترونية، مرجع سابق، ص 283 وما بعدها.
(2) د. عبد الفتاح بيومي حجازي، مقدمة التجارة الإلكترونية العربية، مرجع سابق، ص209.

المبحث الثالث

جريمة التصريح عمدًا بمعطيات خاطئة

يستهدف النص على هذه الجريمة حماية عملية التجارة الإلكترونية وأطرافها من استقبال معلومات خاطئة تؤثر على حقوق أطراف التعاقد البائع والمشتري أو المنتج والمستهلك، أو تؤثر على الثقة المفترضة في هذه التجارة؛ نظرًا لأن المعلومات أو البيانات تلعب دورًا أساسيًا في نجاح التجارة الإلكترونية ومن ثم الإقبال عليها، وما يحمله ذلك من فوائد تنعكس إيجابا أو سلبا على المجتمع الإنساني كله.

أولا: تعريف الجريمة:

تقع هذه الجريمة على بيانات التجارة الإلكترونية، ويهدف التجريم إلى حماية المتعاملين في نطاق هذه التجارة والذين يتعاملون في بياناتها نظرًا لما لها من أهمية ولأن التجارة الإلكترونية تعتمد عليها، فالبيانات أو المعلومات المعالجة تعد عنصرًا جوهريًا فيها؛ لذا فإن التجريم يهدف إلى زيادة الثقة لدى المتعاملين في هذه التجارة والحفاظ على حقوقهم، وقد نصت على هذه الجريمة المادة (27) من قانون المعاملات والتجارة الإلكترونية الإماراتي[1]، حيث عاقبت كل من قدم متعمدًا بيانات غير صحيحة إلى مزود خدمات التصديق بغرض طلب استصدار أو إلغاء أو إيقاف شهادة مصادقة إلكترونية.

---

(1) جاء نص المادة (27) من قانون المعاملات والتجارة الإلكترونية الإماراتي على النحو التالي: (يعاقب بالحبس مدة لا تزيد على ستة أشهر، وبالغرامة التي لا تزيد على مائة ألف درهم، أو بإحدى هاتين العقوبتين كل من قدم متعمدًا بيانات غير صحيحة إلى مزود خدمات التصديق، بغرض طلب استصدار أو إلغاء أو إيقاف شهادة مصادقة إلكترونية).

كما نصت على هذه الجريمة المادة (47) من قانون التجارة والمبادلات الإلكترونية التونسي[1]، والنص يعاقب على جريمة التصريح عمدًا بمعطيات خاطئة من جانب أي شخص سواء لمورد خدمات التوثيق الإلكتروني أو لأي من أطراف العملية التجارية.

وقد نص قانون المعاملات الإلكترونية الأردني على هذه الجريمة أيضًا وبذات الصورة في المادة (36)[2]، وهذا النص لا يوجد ما يقابله في مشروع قانون التجارة الإلكترونية المصري.

ثانيًا: الركن المادي للجريمة:

جريمة التصريح عمدًا بمعطيات خاطئة لمورد خدمات التوثيق الإلكتروني تقتضي إعطاء معطيات غير صحيحة من جانب أي شخص، وهذه المعطيات تتعلق بالطبع بعملية التجارة الإلكترونية محل البحث، على أن يكون التصريح بهذه المعطيات الخاطئة قد صدر إلى مورد خدمات التوثيق الإلكتروني، وهو شخص طبيعي أو معنوي حصل على ترخيص من الجهة المختصة ويصدر شهادات مصادقة لأطراف التعاقد، فهو بمثابة

---

(1) نص قانون التجارة الإلكترونية التونسي في المادة (47) منه على أن: (يعاقب كل من صرح عمدا بمعطيات خاطئة لمورد خدمات التوثيق الإلكتروني ولكافة الأطراف التي طلب منها أن تثق بإمضائه بالسجن لمدة تتراوح بين 6 أشهر وعامين، وبغرامة تتراوح بين 1000، و10.000 دينار أو إحدى هاتين العقوبتين).

(2) نصت المادة (36) من قانون المعاملات الإلكترونية الأردني رقم 85 لسنة 2001 على أن:
(يعاقب كل من يقدم إلى جهة تمارس أعمال توثيق المستندات معلومات غير صحيحة بقصد إصدار شهادة توثيق أو وقف سريانها أو إلغائها بالحبس مدة لا تقل عن شهر ولا تزيد على ستة أشهر، أو بغرامة لا تقل عن (1000) ألف دينار ولا تزيد على (5000) خمسة آلاف دينار، أو بكلتا هاتين العقوبتين).

وسيط لأطراف عملية التعاقد، ويكون مسئولا عن إصدار وتسليم وحفظ تلك الشهادات، واتخاذ الوسائل اللازمة لحمايتها من التقليد والتدليس، ولهذا فعدم صحة البيانات التي يتم الإدلاء بها إليه قد تؤثر على صحة شهادة المصادقة وتؤثر بالتبعية على عملية المصادقة ذاتها.

ويستوي في القانون التونسي أن يكون الإدلاء بهذه المعطيات غير الصحيحة إلى أطراف عملية التعاقد أو أي طرف آخر، كبنك أحد الأطراف مثلا، وكان يتعين على هذا الشخص الالتزام بصحة المعطيات التي صرح بها لثقة مورد الخدمة الإلكترونية وكذلك الأطراف في توقيعه على غير ما صدر عنه، أما المشرع الإماراتي فاشترط لقيام الجريمة أن يكون التصريح لمزود خدمات التصديق, وبغرض طلب استصدار أو إلغاء أو إيقاف شهادة مصادقة إلكترونية, ويكفي لتوافر الركن المادي التصريح من جانب الجاني بهذه المعطيات الخاطئة دون أن يتطلب المشرع تحقيق نتيجة معينة لها، فتعد هذه الجريمة من جرائم السلوك المجرد أو جرائم الخطر وليست من جرائم الضرر [1].

ويتمثل الركن المادي في قيام الجاني أو نائبه بتقديم بيانات غير صحيحة، أيًا كان موضوع هذه البيانات المغلوطة أو الكاذبة إلى مزود خدمات المصادقة الإلكترونية، ويكون الغرض من ذلك استصدار شهادة التصديق الإلكتروني، أو وقف شهادة صادرة وقائمة بالفعل أو إلغاءها.

ويرى جانب من الفقه أن هذه الجريمة تقترب من التزوير في مفهومه التقليدي في نصوص قانون العقوبات المصري والإماراتي، وذلك فيما يتعلق بوضع أسماء أو صور أشخاص آخرين مزورين، فقد ينتحل هوية غيره أو

(1) د. عبد الفتاح بيومي حجازي، الحماية القانونية للتجارة الإلكترونية، مرجع سابق، 287.

إبدال شخصيته، والجاني في هذه الجريمة يقدم متعمدًا بيانات خاطئة وغير صحيحة عن هويته أو تفويضه إلى مزود خدمات التصديق، الذي يصدر شهادات التوثيق المعول عليها[1].

ثالثًا: الركن المعنوي للجريمة:

جريمة الإفضاء بمعطيات غير صحيحة هي جريمة عمدية، تطلب المشرع صراحة توافر القصد الجنائي فيها، حيث نص على أن يكون فعل الإعطاء (عمدًا) فلم يدع مجالا للشك في تحديد ماهية الركن المعنوي، فلا يتصور إذن أن تتحقق الجريمة بصورة غير عمدية، فالإعطاء في حد ذاته يفيد معنى الإرادة والسعي والعلم معًا، وهذه الجريمة لا تتطلب لقيامها قصدًا جنائيًا خاصًا أو نية خاصة لدى الجاني، ولا يتصور وقوعها كذلك بطريق الخطأ.



(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 88, وحول ذلك انظر أيضا: د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، 137, د. خالد محمد المهيري، النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة، مرجع سابق، ص 463.

المبحث الرابع

جريمة التلاعب في بيانات نظم المعلومات

سبق لنا الحديث عن جريمة الدخول غير المشروع للأنظمة المواقع, وجريمة إتلاف البيانات والمعلومات والبرامج, وشاهدنا أن المشرع الفرنسي لا يحمي النظام من الناحية المادية, ولكنه يحمي المعلومات الموجودة بداخل النظام, ضد أي قرصنة معلوماتية[1].

المادة 3/323 من قانون العقوبات الفرنسي الجديد عاقبت كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للبيانات, أو محا أو عدل بطريق الغش تلك المعطيات بعقوبة الحبس حتى ثلاث سنوات وبعقوبة الغرامة حتى ثلاثمائة ألف فرنك.

يتمثل النشاط الإجرامي في هذه الجريمة في أفعال الإدخال أو المحو أو التعديل، ويكفي توافر أحدها لقيام الجريمة، فلا يشترط اجتماعها معًا حتى يتوافر النشاط الإجرامي فيها، ومن ثم قيام الركن المادي في الجريمة، لكن القاسم المشترك في هذه الأفعال جميعها هو انطواؤها على تلاعب في المعلومات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة[2]، ويتم ذلك عن طريق تقنيات الاتصالات الحديثة.

ولذلك فإن السلوك الإجرامي في هذه الجريمة موضوعه محدد، وهو وقوع اعتداء على المعطيات المعالجة، وهي البيانات التي أدخلت لمعالجتها

---

(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق, ص 55.

(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 58.

وتحولت إلى معطيات عبارة عن رموز أو إشارات تمثل تلك المعلومة، أي بيانات تمت معالجتها، فالجريمة في هذا الفرض تقع على المعطيات الناجمة عن البيانات التي تمت معالجتها، دون المعلومة ذاتها، ولذلك يخرج من نطاق هذه الجريمة البيانات التي لم تعالج بعد، ولم تدخل إلى نظام معالجة البيانات، كذلك البيانات التي أدخلت إلى النظام، لكن لم يتم البدء في معالجتها، وكذلك المعلومات التي انفصلت عن النظام وسجلت على شريط ممغنط أو قرص مدمج أو ضوئي، وذلك لأنها أصبحت خارج النظام، والنص يحمي المعلومات المعالجة داخل النظام أو تلك التي في طريقها للمعالجة بأن اتخذت خطوة أو أكثر في مراحل معالجتها[1].

والسلوك الإجرامي في هذه الجريمة يتحقق بطريق فعل الإدخال أو فعل المحو أو فعل التعديل، رغم أن المشرع استخدم مصطلحات مغايرة في نص المادة (2) من قانون مكافحة جرائم تقنية المعلومات الإماراتي، والتي سبق الحديث عنها تفصيلا عند حديثنا عن جرائم الدخول غير المشروع على المواقع والأنظمة، ونعرض هنا لبعض صور السلوك الإجرامي المذكورة في القانون الفرنسي باختصار كما يلي:

أولا: يتحقق فعل الإدخال بإضافة معطيات جديدة على الدعامة الخاصة به، سواء كانت خالية أو يوجد عليها معطيات من قبل[2]، وتقع هذه الجريمة غالبًا بمعرفة المسئول عن القسم المعلوماتي والذي يسند إليه وظائف المحاسبة والمعاملات المالية، لأنه يكون في أفضل وضع يؤهله لارتكاب

(1) د. عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، ص 180.
(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 59.

هذا النمط من التلاعب غير المشروع [1]، ومن الصور العملية لإدخال معلومات مصطنعة قيام المسئول المعلوماتي في المنشأة بضم مستخدَمين غير موجودين بالفعل[2]، أو قيامه بالإبقاء على مستخدَمين تركوا الوظيفة فعلا [3].

ويتحقق فعل الإدخال كذلك في الفرض الذي يمكن فيه الحامل الشرعي لبطاقات السحب الممغنطة، والتي تسحب النقود من البنوك وتحديدًا من أجهزة الحاسب الآلي، وذلك حين يستخدم رقمه الخاص والسري للدخول حتى يسحب مبلغًا من النقود أكثر من المبلغ الموجود في حسابه، أو أن يسدد عن طريقها مبلغًا أكبر من ذلك المبلغ المسموح به لصاحب البطاقة، كذلك يتحقق هذا الفرض عند استخدام البطاقة المذكورة من قبل الغير في

(1) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 71.

(2) المرجع السابق، ص 73.

وأضاف أنه في إحدى الشركات الفرنسية قام أحد مسئولي القسم المعلوماتي باختلاس أكثر من مليون فرنك فرنسي، وأودع هذا المبلغ في حسابه الشخصي وحساب شركائه في العمل الإجرامي، وقد تم ذلك عن طريق قيامه بإعادة ملف المستخدَمين السابقين الذين لهم حقوق مالية، وقام بتحويلها إلى حسابه هو وحسابات أخرى افتتحها خصيصا لهذا الغرض عن طريق شركاء، وبعد تمام الجريمة قام بإصلاح الموقف السابق عن طريق محو كل آثار فعل الغش المعلوماتي، وكان من المستحيل تنفيذ هذه الجريمة دون استخدام حاسب آلي يتلقى أمرا من مشغله بالتغاضي عن بعض المعاملات المالية.

(3) محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 73. يتحقق هذا النمط من الغش المعلوماتي في أن المبرمج المسئول عن الإدارة المعلوماتية بدلا من أن يحفظ الملفات الخاصة بالأشخاص الذين تركوا العمل بالمنشأة فإنه يبقي هذه الملفات نشطة تدر دخلا كل شهر.

حالات سرقتها أو فقدها أو تزويرها، وكذلك عند إدخال معلومات تؤدي إلى إضافة جـديدة[1]، ويلاحظ أن التطور الهائل في تقنية الاتصالات الحديثة تساعد على وقوع هذه الجرائم.

ثانيًا: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة في الحاسب الآلي أو إضافة جزء من المعطيات إلى المنطقة الخاصة بالذاكرة[2].

ويمكن للمسئولين عن حفظ البيانات أن يغيروا ويتلفوا المعلومات المكلفين بحفظها داخل جهاز الحاسب الآلي، وذلك عن طريق إتلاف المعلومات أو محوها[3].

---

(1) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 532, وينظر بعض الأمثلة العملية لدى د. جميل عبد الباقي، الحماية المدنية والجنائية للبطاقات الممغنطة، دار النهضة العربية، القاهرة،1999، ص 88.

(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 59.

(3) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 75. ويذكر أن أحد المستخدمين بمكتب القوى العاملة, وكان مكلفا بتوزيع الإعانات المالية, قام بتحويل مبلغ وقدره (500و000) مارك ألماني لحسابه في شكل مرتبات, وقد أزال من المنفذ الخاص بمساعدة الحاسب الآلي الرقم الأول للمبلغ المحول, وقد حكم عليه بالسجن لمدة ثلاث سنوات، ومن تطبيقات هذه الجريمة بطريقة المحو كذلك قيام بعض المسئولين بالاستيلاء على مبلغ (61.000) دولار كانت قد أرسلتها إحدى شركات التأمين لصالح أحد المراكز الطبية, وقاموا بفتح حسابات وهمية خاصة وضعوا فيها المبلغ, وحتى تتم هذه العملية بنجاح قام هؤلاء المسئولون بمحو بعض الحسابات من سجلات الحاسب الآلي للمركز الطبي، وهى حسابات المتوفين, وذلك بجعلها إما أن تكون غير قابلة للتحصيل أو بحذفها من الملفات، والطريقة ذاتها استخدمت في صناديق المعاشات الألمانية, حيث لاحظت الحكومة أن عددا من المحالين للمعاش يخفى البيان الخاص بهم خلال فترة الصيف، وتفسير ذلك كان أنه بمجرد الإبلاغ عن حالة الوفاة فإن المسئولين =

كما أن محو البيانات المعالجة يمكن أن يتحقق عن طريق التلاعب في الشرائط الممغنطة، ففي فرنسا اكتشفت عملية نصب بطريق التلاعب في الشرائط الممغنطة قدرت قيمتها بحوالي (21) مليون فرنك فرنسي بسبب الخطأ المعلوماتي[1].

واختلف الفقه في شأن تصنيف هذه الواقعة، إذ لا تجد سندها في المادة (323- 3) من قانون العقوبات الفرنسي، التي تجرم الاعتداء على المعلومات في داخل نظام معالجة المعلومات، أما تلك التي لم تدخل بعد أو دخلت وانفصلت عن النظام فالحماية الجنائية قد تتوافر تحت مظلة نصوص أخرى كتلك النصوص التي تعاقب على التعييب أو الإتلاف المادي للوسائط

= المختصين عن النظام المعلوماتي للمعاشات يغيرون عناوين المتوفين حتى لا يمكن استدعاؤها إلى الإدارة الخاصة بالمراقبة, وبالتالي يقوم المسئول عن نظام المعاشات بتوجيه الشيكات الخاصة بالمحالين للمعاش, لاسيما وأنه يجب على الألماني أن يتقدم إلى صندوق المعاشات مرة واحدة خلال الصيف.
كذلك فقد تم الكشف في مدنية دالاس الأمريكية عن أربعة أشخاص من مستخدمي البلدية كانوا قد استبعدوا (271) مخالفة من السجلات المدنية مقابل تقاضي نسبة محددة بلغ مجموعها (16300) دولار.

(1) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، مرجع سابق، ص 76، وفي المعنى ذاته: د. جميل عبد الباقي، الحماية المدنية والجنائية للبطاقات الممغنطة، مرجع سابق، ص 34.

- وتخلص وقائع الدعوى في أنه بتاريخ 29 فبراير 1981 وصل إلى أحد فروع الشركة العامة شريط ممغنط قادم من شركة تدعى isaver, وقد احتوى هذا الشريط على (139) إذنا بالدفع, وعند معالجته بالقسم المعلوماتي للبنك رفض بواسطة الحاسب الآلي بسبب عيب جسيم يتعلق بطول تسجيل الشريط, وألقي القبض على الجاني الذي وجهت إليه تهمة التعييب, وكان بالإمكان نجاح هذه المحاولة لو توافر لدى المزيف المعرفة المعلوماتية والتقنية اللازمة في المجال المعلوماتي.

المعلوماتية[1].

ثالثًا: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، إذ إنه قد يتم التلاعب في المعطيات عن طريق استبدال هذه المعطيات، أو عن طريق التلاعب في البرامج وذلك بإمداد البرنامج بمعطيات مغايرة عن تلك التي صمم البرنامج لأجلها[2]، والقاعدة العامة أن المحو والتعديل للمعطيات الموجودة في النظام كصورتين للركن المادي في جريمة الاعتداء على نظام المعالجة الآلية للمعطيات يتحققان عن طريق برامج تتلاعب في هذه المعطيات، وذلك بمحوها كليًا أو جزئيًا أو بتعديلها باستخدام القنبلة المعلوماتية الخاصة بالمعطيات سواء كانت منطقية أم زمنية، وكذلك عن طريق برامج المحو أو برامج الفيروسات بصفة عامة، لاسيما وأن الفيروس المعلوماتي يصنعه مجرم معلوماتي على درجة عالية من الذكاء، ذو قدرة عالية في تقنية المعلومات[3].

وتقوم هذه الجريمة على القصد الجنائي العام بركنيه العلم والإرادة، ذلك

(1) وقد قضي في فرنسا بأنه لا يشترط في المحو أو الإلغاء المعاقب عليه بالمادة (1/323) عقوبات فرنسي- أن يرتكب بواسطة شخص ليس له حق الدخول في نظام ولا يشترط حتى أن يكون الشخص لديه نية الضرر.
د. خالد المهيري، النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة، مرجع سابق، ص 567.

(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 59, وفي المعنى ذاته: د. جميل عبد الباقي، الحماية المدنية والجنائية للبطاقات الممغنطة، مرجع سابق، ص 34.

(3) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 60, وفي المعنى ذاته: د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص 359.

أنه يجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، وأن يعلم أن نشاطه غير مشروع، وأنه يتعدى على صاحب الحق في المعطيات، ومع ذلك تتجه إرادته إلى ذلك الفعل رغمًا عن إرادة صاحب الحق في المعطيات أو من له السيطرة عليها[1]، ولا تتطلب هذه الجريمة قصدًا جنائيًا خاصًا، ذلك أن الركن المادي في هذه الجريمة يقوم بمجرد توافر فعل الإدخال أو المحو أو التعديل، ويتوافر الركن المعنوي بانصراف القصد الجنائي إلى فعل من هذه الأفعال[2].



(1) د. مدحت رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 56 , وفي المعنى ذاته، مرجع سابق، ص 60.

(2) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص 60.

المبحث الخامس

الاعتداء على نطاق أسماء الدومين

يتشابه نظام أسماء الدومين في الوظيفة مع دليل الهاتف من حيث إنه يسمح بتمييز صاحب الاسم المستخدم لجهاز حاسب معين بحيث يمكن الوصول إلى موقعه الإلكتروني دونًا عن غيره، وبالتالي تبادل البيانات والمعلومات بين أصحاب المواقع المسماة بأسماء مميزة دونما اختلاط أو تعثر، ويطلق نظام أسماء الدومين على مجموعة الحروف والأرقام والرموز التي يتم تسمية الموقع بها، والأساس الذي يتم الوصول به إلى الموقع هو أساس رقمي، أما الاسم فليس إلا نظامًا مضافًا يسمح بتيسير التعرف على الموقع الذي تم تعيينه على أساس الأرقام، وفي النهاية فهو الاسم الذي يدخل المستخدم عن طريقه إلى شبكة الإنترنت لغرض ما وقد يكون الدخول لغرض تجاري من شركة أو مؤسسة أو مجموعة اقتصادية، وهو ما يستلزم حمايته ووضع ضوابط لتسجيله.

أولا: أسماء الدومين في القانون الإماراتي والمشروع المصري:

قانون المعاملات والتجارة الإلكترونية لدولة الإمارات لم يبد أي اهتمام بموضوع حماية الدومين وأسماء الحقول، وتركها للقواعد العامة المعمول بها، وكذا القانون المحلي لإمارة دبي[1].

---

(1) اهتم قانون التجارة الإلكترونية البحريني بموضوع تسجيل أسماء النطاق، فنصت المادة (21) منه على أنه:
1- لوزير المواصلات أن يصدر قرارًا بتنظيم تسجيل واستعمال اسم النطاق لمملكة البحرين (bh) والترخيص باستعماله أو حظر ذلك، بعد أخذ رأي وزير التجارة والصناعة وأي شخص يكون من المناسب استطلاع رأيه في هذا الشأن، بما في ذلك مؤسسة الإنترنت للأسماء والأرقام المعينة. =

وعلى العكس من ذلك اهتم مشروع قانون التجارة الإلكترونية المصري بموضوع أسماء الدومين وحمايته، نظرًا لأهميته في مجال التجارة الإلكترونية، ونظرًا لأن كل موقع أو اسم دومين إنما يعبر عن مؤسسة اقتصادية أو تجارية بما يستلزم حمايته وتسجيله، ووضع المشروع مبدأين:

المبدأ الأول: تختص جهة معينة بمنح التراخيص نظير رسم، والجهة في مصر- هي مركز المعلومات ودعم اتخاذ القرار التابع لرئاسة مجلس الوزراء المصري، منعًا لتكرار أسماء الدومين، ولمنع الاعتداء على حقوق الأسماء سابقة التسجيل.

المبدأ الثاني: احترام أسبقية التسجيل لاسم الدومين، ما لم يكن الأسبق للتسجيل سيء النية فيفقد حقه في التسجيل لسوء نيته، وهنا يتشابه تنظيم

= (Assigned Names and Numbers Internet Corporation)

2- يجوز أن يتضمن القرار الصادر بتنظيم تسجيل واستعمال اسم النطاق ما يلي:

أ- إنشاء مكتب لتسجيل اسم النطاق يتبع وزارة المواصلات.

ب- البيانات التي يتضمنها طلب التسجيل.

ج- مدة سريان التسجيل.

د- الشروط والإجراءات والمدة المتعلقة بإعادة التسجيل.

هـ- الشروط والإجراءات المتعلقة بمنح التسجيل.

و- إجراءات التظلم من القرارات الصادرة من مكتب تسجيل اسم النطاق.

ز- تحديد فئات الرسوم المستحقة على طلب التسجيل أو تجديده أو إعادة التسجيل، وطريقة سداد هذه الرسوم بعد موافقة مجلس الوزراء.

ح- أية مسائل أخرى متعلقة بالتسجيل.

3- يقصد باسم النطاق (bh) فيما يتعلق بتطبيق أحكام هذه المادة، المستوى العلوي للنظام العالمي لاسم النطاق المعين لمملكة البحرين، والذي يتكون من حرفين وفقا للمعيار الدولي أيزو 1، 3166 (رموز تمثيل أسماء البلدان وتقسيماتها الفرعية) الخاص بالمنظمة الدولية للتقييس.

اسم الدومين مع تنظيم الأسماء والعلامات التجارية.

ثانيًا: صور الاعتداء على أسماء الدومين:

الصورة الأولى: الاعتداء من خلال تطابق الاسم.

الصورة الثانية: الاعتداء من خلال تشابه الاسم بما يؤدي إلى تضليل المستهلك أو الوسطاء، والمعيار الذي يتخذه القضاء في ذلك هو معيار الرجل المعتاد.

الصورة الثالثة: استخدام اسم الدومين للإساءة إلى إحدى السلع أو الخدمات أيًا كان تاريخ تسجيل الاسم.

الصورة الرابعة: احتجاز الأسماء المشهورة أو المشابهة لهذه الأسماء بهدف إعادة التصرف فيها، بما يهدد مصالح أصحاب الأسماء.

ولا تتوقف منازعات أسماء الدومين على الصور التقليدية التي سبق عرضها، فالحقيقة أن التقنيات الحديثة قد أدت إلى استحداث منازعات لم تكن مألوفة من قبل، وأضافت أبعادًا حديثة لمنازعات تقليدية.

ومن ذلك على سبيل المثال تحديد النطاق المكاني لتطبيق القانون الوطني بشأن المنازعات التي يثيرها الاعتداء على الأسماء والعلامات التجارية، ذلك أن الاعتداء على الاسم أو العلامة التجارية لإحدى السلع المشهورة في دولة معينة قد يقتضي إعمال قانون هذه الدولة بشأن معاملة تجارية يقيم أحد أطرافها في دولة أخرى، كما هو الشأن على سبيل المثال في الحالات التي يتمسك فيها المشتري بإبطال العقد أو التعويض استنادًا إلى ما تسبب فيه اللبس الناجم عن استخدام اسم مشابه أو مطابق للاسم أو العلامة التجارية الشهيرة من إقدامه على الشراء من البائع الذي اعتدى على هذا الاسم أو هذه العلامة.

كذلك فإن حماية المشتري (المستهلك) نفسه قد تقتضي تطبيق

تشريعات الحماية المقررة لمصلحته في قانون الدولة التي كان يرغب في شراء السلعة المنتجة فيها، بالرغم من أن الاعتداء على الاسم قد وقع على المستوى الأعلى لاسم الدومين **TLD** في دولة أخرى.

وهكذا تحتاج الفروض السابقة إلى النظر في قواعد الإسناد والإحالة من ناحية، وتحديد نطاق تطبيق القانون الوطني من ناحية أخرى في ضوء طبيعة التعامل التجاري من خلال شبكة الإنترنت.

كذلك فإن الاعتداء التقليدي على الاسم والعلامة التجارية لم يصبح الصورة الوحيدة التي يجب حمايتها، وإنما ظهرت صور جديدة من الاعتداءات تستحق الحماية بذات القدر والدرجة، من ناحية أخرى فإن اللجوء إلى أجهزة البحث لوضع أسس ومعايير تصنيف الأسماء محل البحث "المطابقة المتشابهة" قد يؤدي إلى إهدار شهرة إحدى العلامات الشهيرة، أو الإيهام بتفضيل إحدى السلع على الأخرى نتيجة تقدمها في الترتيب، وما يسمح به نظام الربط استنادًا إلى أسماء الدومين من استظهار أسماء متطابقة أو متشابهة أو مختلفة على ذات الصفحة، بما قد يوحي للمستهلك بوجود ارتباط أو صلة تعاقدية بين أصحاب هذه الأسماء التي تعمل في النشاط ذاته.

كما أن الإطارات التي تظهر فيها مواقع الإعلانات التجارية قد تؤدي للخلط بين صاحب الاسم والعلامة التجارية التي يبحث عنها المستهلك وبين صاحب الاسم المعلن عنه، وقد يكون ذلك مقصودًا بما يؤدي إلى الإضرار بصاحب الاسم أو العلامة التجارية، وهو ما يدعو إلى البحث عن المبادئ والقواعد المنظمة لمثل هذه العلاقات والمحققة لحماية المضرور من هذه الممارسات.[1]

(1) د. حسن عبد الباسط جميعي، الحماية القانونية لمواقع الإنترنت وأسماء الدومين،=

وهناك أوجه تشابه بين اسم الدومين والعلامة التجارية من حيث إن كليهما يعبر عن منتجات - سواء أكانت خدمة أم سلعة - منسوبة إلى مؤسسات معينة، كما أن المعيار المتبع في حماية العلامات التجارية هو أسبقية التسجيل، وهو المعيار نفسه الذي تم اتباعه في تسجيل أسماء الدومين، كما أن العلامات التجارية يشترط فيها شروط ثلاثة، هي أن تكون مميزة وجديدة ومشروعة، وكذلك أسماء الدومين، والعلامات التجارية يشترط تسجيلها، وكذلك أسماء الدومين[1].

ثالثًا: النظام القانوني لحماية أسماء الدومين:

يمكن لمقدم الخدمة أن يضع في العقد المبرم مع المستخدم نصوصًا منظمة لاختصاصه (أي مقدم الخدمة) بالفصل في المنازعات الخاصة بأسماء الدومين، ونظرًا إلى عدم كفاية هذا النظام، وكذلك بالنظر إلى غياب تنظيم تشريعي خاص بهذا النوع من أنواع المنازعات، فإن القضاء في أمريكا وأوروبا قد اتجه إلى إعمال النصوص التشريعية والقواعد العامة المطبقة في حماية الأسماء والعناوين والعلامات التجارية، كذلك فإن الحماية المقررة للأسماء والعلامات التجارية ترتبط أيضًا بما ورد من نصوص في التشريعات الخاصة بحماية المستهلك وبتنظيم المنافسة ومنع الاحتكار.

وهكذا فإنه في ظل الوضع الحالي وحتى يتم وضع نصوص تشريعية

= بحث مقدم لندوة الويب الوطنية عن الملكية الفكرية التي نظمتها المنظمة العالمية للملكية الفكرية الوايبو بالتعاون مع جامعة القاهرة (مصر) في الفترة من 17 إلى 19 فبراير 2003، ص 18 وما بعدها.

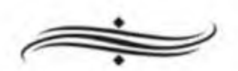
(1) د. هدى حامد قشقوش، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، مرجع سابق، ص 83.

خاصة بتنظيم حماية أسماء الدومين، فإن المنازعات الخاصة بأسماء الدومين وبالأسماء والعناوين والعلامات التجارية تحكمها المبادئ العامة والنصوص التشريعية المنظمة للحماية في هذه المجالات الأخيرة، مع ضرورة أن يتم تسجيل أسماء الدومين بوصفها اسمًا أو عنوانًا أو علامة تجارية لتأكيد وتأمين هذه الحماية بعيدًا عن اجتهاد الفقه والقضاء اللذين لم يتبنيا حتى الآن موقفًا مشابهًا لما استقر عليه القضاء في أمريكا أو فرنسا أو غيرهما من البلاد الأوروبية.

هذا وقد يؤدي الاعتداء على الاسم والعلامة التجارية بواسطة تسجيل اسم الدومين إلى قيام المسئولية المدنية استنادًا إلى قواعد المسئولية التقصيرية وقواعد المنافسة التجارية غير المشروعة.

أما المسئولية الجنائية فلا نعتقد أن إعمال القواعد العامة وقياس حكم هذه الحالة المسكوت عنها على الحالات المنصوص عليها يسمح بتطبيق النص الجنائي، حيث إن النص الجنائي لا يتوسع في تفسيره أو في تطبيقه احترامًا للمبدأ الأساسي "لا جريمة ولا عقوبة إلا بنص صريح".

وهكذا وما لم يتم تسجيل اسم الدومين كاسم تجاري أو كعلامة تجارية في السجل المخصص لذلك، فإنه في ظل القانون الحالي لا يمكن تطبيق أحكام القواعد العامة ونصوص الحماية إلا من خلال قواعد المسئولية المدنية دون قواعد المسئولية الجنائية.



الفصل الثالث

الجرائم الواقعة على وسائل التجارة الإلكترونية

تمهيد وتقسيم:

تمثل الجرائم الواقعة على وسائل التجارة الإلكترونية اعتداءً على جوهر التجارة الإلكترونية، من حيث العقود الإلكترونية المبرمة، ومدى حجية التوقيع الإلكتروني، وإمكان تزويره، والاعتداء على وسائل الدفع الإلكتروني، والتي تمس أطراف العلاقة في التجارة الإلكترونية، وتمس كذلك شهادات المصادقة الصادرة من مزود الخدمة[1].

وتعتبر الكتابة من أهم وسائل الإثبات جميعها، لما توفره للخصوم من ضمانات، كما أن التوقيع على الورقة يتضمن قبول المكتوب بها، واعتماد محتواها كدليل إثبات[2]، وتستبدل الكتابة التقليدية بكتابة إلكترونية في مجال إبرام عقود التجارة الإلكترونية[3]، كما يستبدل التوقيع التقليدي بتوقيع إلكتروني لكل من مقدم الخدمة أو البائع، ومتلقي الخدمة أو المستهلك، فتبرم العقود بدون تواجدهم في مكان التعاقد[4].

ونظرًا لما يحمله التوقيع الإلكتروني من أهمية فقد تبنى القانون

(1) د. نزيه محمد الصادق المهدي، النظرية العامة للالتزام، دراسة نظرية تطبيقية في مبادئ الإثبات، دار النهضة العربية، القاهرة، طبعة 2001، ص 32.

(2) د. ثروت عبد الحميد، التوقيع الإلكتروني، مرجع سابق، ص 9.

(3) Loma Brazell: Electronic signatures law and regulations. SWEET AND MAXWELL،London،2004،p54

(4) European commission: Digital signatures A survey of law and practice in the European union، Wood DHEAD publishing LIMITED، Cambridge England،2001،p69

النموذجي بشأن التوقيعات الإلكترونية مبدأ الحياد التقني[1]، فركزت مجموعة العمل التي أعدت هذا القانون جهودها على تنظيم التوقيع الإلكتروني الرقمي المستند إلى نظام التشفير غير المتماثل، باعتباره أكثر الأنواع انتشارًا، حيث يمكن أن تتدخل جهة التصديق لكي تبعث الثقة فيما تصدره من شهادات، وما تفرضه على المتعاملين من التزامات في التوقيعات الإلكترونية.

واهتمت التشريعات بحماية هذا التوقيع جنائيًا فأصدر المجلس الأوروبي في 13 ديسمبر 1999 التوجيه رقم (1999/93) الخاص بإنشاء إطار قانوني للتوقيعات الإلكترونية، وخدمات المصادقة، بهدف تسهيل استعمالها، والاعتراف القانوني بها، واستلزمت المادة الثانية/1 أن يكون التوقيع الإلكتروني مرتبطًا بموقع التجارة الإلكترونية، وقادرًا على تحديد هوية الموقع، وينشأ باستخدام وسائل خاصة بالموقع، وأن يكون مرتبطًا بالبيانات التي يشير إليها[2].

وفي القانون رقم 2006/1 بشأن التجارة الإلكترونية بدولة الإمارات العربية المتحدة يعرف التوقيع الإلكتروني بأنه: " توقيع مكون من حروف أو أرقام أو رموز أو صوت أو نظام معالجة ذو شكل إلكتروني، وملحق أو مرتبط منطقيًا برسالة إلكترونية، وممهور بنية توثيق أو اعتماد تلك الرسالة".

ونظرًا لارتباط التوقيع الإلكتروني بعقود التجارة الإلكترونية، واعتباره

---

(1) د. محمد أحمد محمد نور جستنية، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 2005، ص 39.

(2) Reedc: What is a signature?:2000(3)The Journal of information.Law and Technology (JILT)
"http:www.elj.warwick.ac.uk\jilt\00،3reed.htmll"

إحدى الوسائل المهمة لها بالإضافة إلى الوسائل الأخرى كالدفع الإلكتروني، ووسائل المصادقة الإلكترونية، فإننا سنتناول في هذا الفصل، الاعتداء على التوقيع الإلكتروني، وجرائم إساءة استخدام بطاقات الدفع الإلكتروني، والجرائم المتعلقة بمزود خدمة المصادقة الإلكترونية وذلك وفق المباحث التالية:

المبحث الأول: الاعتداء على التوقيع الإلكتروني.

المبحث الثاني: جرائم إساءة استخدام بطاقات الدفع الإلكتروني.

المبحث الثالث: الجرائم المتعلقة بمزود خدمة المصادقة الإلكترونية.



المبحث الأول

الاعتداء على التوقيع الإلكتروني

تتسم التجارة الإلكترونية عبر شبكة الإنترنت بغياب المتعاقدين وعدم حضورهم مباشرة في مجلس العقد، ولكن يتم الاتصال فيما بينهم عبر الشبكة المعلوماتية، ويتم التوقيع من جانبهم إلكترونيًا من خلال وسيلة الاتصال التي يتم من خلالها التعاقد[1]، وقد سبق أن قمنا بتعريف التوقيع الإلكتروني بأنه ملف رقمي أو شهادة رقمية معترف بها تصدر عن إحدى الهيئات المختصة والمستقلة، وفي هذا الملف يتم تخزين الاسم، وبعض المعلومات المهمة الأخرى، مثل رقم التسلسل، وتاريخ انتهاء الشهادة ومصدرها، وتحتوي هذه الشهادة عند تسليمها على مفتاحين (المفتاح العام، والمفتاح الخاص)، ويعتبر المفتاح الخاص هو التوقيع الإلكتروني الذي يميز صاحبه عن بقية الناس، أما المفتاح العام فيتم نشره في الدليل وهو متاح للعامة من الناس للتعامل مع صاحبه[2].

---

(1) Angel J:why use Digital signatures for Electronic commerce? Commentary 1999، the journal of information،Law and Technology (JIL T)، p3 "http://eli.warwick.ac.uk\Jilt\199،2\angel.html"

(2) http: // safola.com/signature.chtml

كما قرر البعض أنه: (مجموعة من الإجراءات التقنية التي تسمح بتحديد شخصية من تصدر عنه هذه الإجراءات، وقبوله بمضمون التصرف الذي يصدر التوقيع بمناسبته).

Jonathan Rosenar CyberLaw. The law of the internet،ed springer، 1997، p.237

كما تم تعريفه بأنه: (وحدة قصيرة من البيانات التي تحمل علاقة رياضية مع=

كما عرف التوقيع الإلكتروني بأنه عبارة عن: (ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع متفرد يسمح بتحديد شخص الموّقع ويميزه عن غيره) وفقًا للتعريف الوارد في قانون التوقيع الإلكتروني المصري رقم 2004/15[1].

وسوف نركز على قانون التوقيع الإلكتروني المصري في هذا المبحث، وعلى أهم الجرائم الواردة فيه، باعتباره قانونًا متخصصًا في التوقيع الإلكتروني، ويكاد يكون القانون العربي الوحيد المتخصص في التوقيع الإلكتروني، وذلك على اعتبار أن التوقيع الإلكتروني ورد ضمن قوانين التجارة الإلكترونية الصادرة كالقانون الإماراتي، والتونسي، والأردني، والبحريني، والعماني.

وقد اهتم قانون التوقيع الإلكتروني المصري بتجريم العديد من صور الاعتداء على هذا التوقيع، وذلك في نص المادة (23) حيث سلك مسلك التشريعات المقارنة الأوروبية والعربية في شأن حماية التوقيع الإلكتروني جنائيًا، للمحافظة عليه من المساس به عن طريق تقليده أو تزويره، وكذلك الأوراق المتصلة بالمعاملة الإلكترونية التي يتم التصديق عليها، كأن يقوم أحدهم بتزويرها.

وتنص المادة (23) من قانون التوقيع الإلكتروني المصري على ما يلي:

= البيانات الموجودة في محتوى الوثيقة) د. عايض راشد المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود التجارية، مرجع سابق، ص 91.

(1) صدر القانون رقم 2004/15 بشأن التوقيع الإلكتروني، ونشر بالجريدة الرسمية بالعدد رقم 17 بتاريخ 2004/4/22، وكذلك اللائحة التنفيذية له الصادرة بقرار وزير الاتصالات وتكنولوجيا المعلومات والمنشور بالوقائع المصرية بالعدد رقم 115 تابع في 2005/5/25.

(مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

أ) أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.

ب) أتلف أو عيّب توقيعًا أو وسيطًا أو محررًا إلكترونيًا، أو زوّر شيئًا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر.

ج) استعمل توقيعًا أو وسيطًا أو محررًا إلكترونيًا معيبًا أو مزورًا مع علمه بذلك.

د) خالف أيًا من أحكام المادتين (19)، (21) من هذا القانون[1].

هـ) توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته.

وتكون العقوبة على مخالفة المادة (13) من هذا القانون الغرامة التي لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه.

وفي حالة العود تزاد بمقدار المثل العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى.

(1) وذلك بأن يتم التوقف عن مزاولة نشاط التصديق الإلكتروني، أو الاندماج في جهة أخرى أو التنازل عن الترخيص للغير، دون الحصول على موافقة كتابية مسبقة من هيئة تنمية صناعة تكنولوجيا المعلومات، أو أن تصدر الجهات الأجنبية شهادات تصديق إلكتروني معترف بها في مصر، دون اعتمادها من هيئة تنمية صناعة تكنولوجيا المعلومات، ودون سدادها الرسوم المقررة والتي يحددها مجلس إدارة هيئة تنمية صناعة تكنولوجيا المعلومات.

وفي جميع الأحوال يحكم بنشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الإلكترونية المفتوحة على نفقة المحكوم عليه).

وسوف نتناول الحماية الجنائية للتوقيع الإلكتروني وفقًا لما ورد في قانون التوقيع الإلكتروني المصري فيما يلي:

1 - جريمة إصدار شهادات التوقيع الإلكتروني بدون ترخيص:

نص القانون في المادة (23) على أنه: (مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

أ) أصدر شهادة تصديق إلكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.

الجريمة الواردة في هذه المادة يتحقق السلوك الإجرامي فيها بانتحال الجاني صفة مزود خدمات التصديق المرخص له بمزاولة العمل وذلك على خلاف الحقيقة، ويقوم بإصدار شهادات تصديق إلكتروني دون ترخيص بذلك من الهيئة المختصة.

وتقوم الجريمة بقيام المؤسسة أو الفرد بإصدار شهادة تصديق إلكترونية وهو غير حاصل على تصريح، أي أنه زاول فعل الإصدار فعلا، أما لو كان مجرد إعلان عن نيته إصدار شهادات توثيق إلكتروني فلا تقوم به الجريمة، أي يجب أن تكون الشهادة قد صدرت من الجاني حقا، وهذه الشهادة هي الدليل على مباشرة الجاني إصدار شهادة توثيق إلكتروني دون ترخيص[1].

(1) Warwick Ford and Michael S.Baum: Secure electronic commerce Building the Infrastructure for Digital signatures and Encryption، prentice Hall ptr، New Jersey،2001،p3.

وشهادة التصديق هي الشهادة التي تصدر من الجهة المرخص لها بالتصديق وتثبت الارتباط بين الموقّع وبيانات إنشاء التوقيع[1]، ومن هذا التعريف يتضح لنا أهمية شهادة المصادقة والسبب الذي جعل المشرع يضفي عليها الحماية الجنائية، إضافة إلى الآثار الخطيرة التي تمس أطراف التجارة الإلكترونية.

والجريمة الواردة في هذه المادة من الجرائم العمدية التي يتحقق ركنها المعنوي في القصد الجنائي العام المتمثل في العلم والإرادة، فيكفي أن يعلم الجاني أن سلوكه المتمثل في إصدار الشهادة دون الحصول على ترخيص يخوله ذلك وفقًا للقانون هو سلوك مجرم، وأن تتجه إرادته للقيام بهذا السلوك المجرم.

ويلاحظ أن هذه الجريمة لا تقع بطريق الخطأ؛ لأن صياغة الفقرة (أ) من المادة المذكورة والتي جرمت الفعل بدأت بعبارة: " أصدر شهادة تصديق إلكتروني " بما يفيد العمد وانصراف الإرادة إلى هذا الفعل[2].

2 - جريمة إتلاف وتزوير التوقيع أو الوسيط أو المحرر الإلكتروني:

الفقرة (ب) من المادة (22) نصت على عقوبة لمن (أتلف أو عيّب توقيعًا أو وسيطًا أو محررًا إلكترونيًا، أو زوّر شيئًا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر).

(1) وفقا لتعريف شهادة المصادقة الإلكترونية الوارد في المادة (1) من قانون التوقيع الإلكتروني المصري رقم 15 لعام 2004.

(2) د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم المقارنة، مرجع سابق، ص 541.

وتتعدد صورة السلوك المجرم في هذه الحالة، فتقوم الجريمة في حالة إتلاف أو تعييب المحرر أو الوسيط أو التوقيع الإلكتروني، أو في حالة تزوير التوقيع الإلكتروني أو المحرر الإلكتروني أو الوسيط بأي طريق كان كالاصطناع أو التعديل أو التحوير.

والمحرر الإلكتروني - وفقًا للتعريف الوارد في القانون - هو رسالة تتضمن معلومات تنشأ أو تدمج، أو تخزن، أو ترسل أو تستقبل كليًا أو جزئيًا بوسيلة إلكترونية أو رقمية أو ضوئية أو بأية وسيلة أخرى مشابهة، أما الوسيط الإلكتروني فهو أداة أو أدوات أو أنظمة إنشاء التوقيع الإلكتروني.

وفعل الإتلاف يتحقق بإفقاد البرنامج المعلوماتي الخاص بالتوقيع الإلكتروني - بأي وسيلة كانت - كليًا قدرته على العمل، أما التعييب فهو الإفقاد الجزئي لهذا البرنامج الخاص بالتوقيع الإلكتروني أو بالوسيط أو بالمحرر الإلكتروني.

وإلى جانب صورتي الإتلاف والتعييب فقد نص القانون على صورة أخرى وهي تزوير التوقيع أو الوسيط أو المحرر الإلكتروني بأي طريقة كانت، كالاصطناع أو التقليد أو التحوير، وهذه الطرق ذكرت في المادة على سبيل الحصر، ويتمثل التزوير هنا في تغيير الحقيقة في محرر بإحدى الطرق التي بينها القانون.

ويقوم الركن المعنوي بعنصريه العلم والإرادة، فهي من الجرائم العمدية التي لا تتوقف فيها العقوبة على تحقيق نتيجة معينة[1].

(1) د. ثروت عبد الحميد، التوقيع الإلكتروني، ماهيته، مخاطره كيفية مواجهتها، مدى حجيته في الإثبات، مكتبة الجلاء، المنصورة، طبعة 2001، ص 9، وفي المعنى ذاته: د. سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته، صوره، حجيته في =

= الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة للنشر، الإسكندرية، 2004، ص 3.

ولكون هذه الجريمة من الجرائم العمدية فيتحقق ركنها المعنوي في صورة القصد الجنائي العام في صورتي الإتلاف والتعييب، والقصد الخاص في التزوير.

وعلى ذلك لابد أن يعلم الجاني حال ارتكابه لجريمة الإتلاف أو التعييب أو التزوير أن هذا الفعل محظور ومعاقب عليه، ومع ذلك يقبل القيام به وتتجه إرادته للفعل ويقبل النتائج المترتبة عليه.

هذا فضلا عن اشتراط توافر القصد الخاص في جريمة تزوير المحرر الإلكتروني أو الوسيط الإلكتروني أو التوقيع الإلكتروني[1].

3 - جريمة استعمال توقيع أو وسيط أو محرر إلكتروني مزور:

المادة (23) من قانون التوقيع الإلكتروني المصري نصت في فقرتها (ج) على جريمة أخرى وعاقبت كل من: (استعمل توقيعًا أو وسيطًا أو محررًا إلكترونيًا معيبًا أو مزورًا مع علمه بذلك).

وتعد هذه الجريمة مرتبطة بالجريمة السابق بيانها والمنصوص عليها في الفقرة (ب) من هذه المادة والخاصة بجريمة إتلاف أو تعييب أو تزوير التوقيع الإلكتروني أو الوسيط الإلكتروني أو المحرر الإلكتروني.

فقد عاقبت هذه المادة من يقوم باستعمال المحرر أو الوسيط أو التوقيع الإلكتروني المعيب أو المزور دون التالف، على اعتبار أن الإتلاف قد أنهى قيمته، أما المعيب فإنه يؤدي وظيفته ولكن بطريقة منقوصة، ولكنه يرتب آثارًا قانونية، ولا يجوز استعماله لأن المشرع يمنع ذلك.

(1) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 181.

والسلوك الإجرامي في هذه الجريمة يتمثل في استعمال ذلك المحرر أو الوسيط أو التوقيع الإلكتروني، وقيام الجاني بإبراز هذا المحرر أو التوقيع الإلكتروني المعيب أو تقديمه إلى الغير بأي طريقة كانت، ويشترط أن يعلم أن هذا المحرر أو التوقيع مزوران.

والركن المعنوي المطلوب هنا هو ذلك القصد الجنائي العام المتمثل في العلم والإرادة، أي أن يكون الجاني عالمًا بأن ما يستعمله من محرر أو توقيع أو وسيط إلكتروني معيب أو مزور، وأن تتجه إرادته إلى فعل الاستعمال المجرم وقبول النتائج المترتبة على ذلك[1].

4 - جريمة الحصول بطريق غير مشروع على التوقيع أو الوسيط أو المحرر الإلكتروني:

الفقرة (هـ) من المادة (23) عاقبت كل من (توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، أو اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته).

يعاقب المشرع في هذه المادة على صورتين من السلوك الإجرامي، الأولى الحصول على توقيع أو وسيط أو محرر إلكتروني بصورة غير مشروعة، وبأية وسيلة كانت كالاحتيال أو السرقة أو غيرها من الطرق غير المشروعة.

والصورة الثانية هي اختراق هذا الوسيط الإلكتروني أو اعتراضه أو تعطيله عن أداء وظيفته[2].

(1) د. عبد الفتاح بيومي حجازي، التوقيع الإلكتروني في النظم المقارنة، مرجع سابق، ص 552.

(2) Mohan Atreya and Benjamin Hammond and Stephen Paine and paul starret and Stephen Wu: Digital signatures ،McGraw،Hill\Osborne،New York،2002،P5

ووفقًا لهذا النص فإن الركن المادي للجريمة يقع على توقيع أو محرر أو وسيط إلكتروني، وقد يتحقق ذلك بالدخول إلى نظام معلومات أو قاعدة بيانات تتعلق بالتوقيع الإلكتروني ذاته، وقاعدة البيانات يراد بها البيانات المخزنة عن موضوع ما في الحاسب الآلي أو على قرص منفصل، ومثالها البيانات المتعلقة باسم صاحب التوقيع ومهنته، أو بياناته الشخصية، أما النظام المعلوماتي فهو بيانات ومعلومات تم معالجتها باتباع طرق إلكترونية حتى صارت برنامجًا تطبيقيًا محملا على الحاسب الآلي لتشغيله والحصول على نتائج معينة خاصة بالتوقيع الإلكتروني، وتتعلق قاعدة البيانات والنظام المعلوماتي بالتوقيع الإلكتروني.

ولم يشترط المشرع في هذه الجريمة تحقق نتيجة معينة على إثر توصل الجاني بأي وسيلة كانت إلى الحصول بغير حق على توقيع أو وسيط أو محرر إلكتروني، أو دخول الجاني بالاختراق لهذا الوسيط والتي يتمثل في قاعدة البيانات ونظم المعلومات أو اعتراضه أو تعطيله عن أداء عمله بصورة سليمة.

ولم يعتد المشرع هنا بطريقة الدخول أو الاختراق، أو كيفية الحصول على هذا التوقيع، فتقع الجريمة بأية طريقة كانت للحصول عليه بغير حق، وعلى ذلك فإن هذه الجريمة تعد من جرائم الخطر ولست من جرائم الضرر، بمعنى أن العقوبة تقع على السلوك الإجرامي دون اشتراط تحقق نتيجة معينة، ولا تقع الجريمة إذا كان الدخول بناءً على إذن قضائي، أو من قبل الأشخاص المصرح لهم بالاطلاع على النظام المعلوماتي أو قاعدة البيانات المتعلقين بالتوقيع الإلكتروني[1].

(1) Warwick Ford and Michael S.Baum: Secure electronic commerce Building the Infrastructure for Digital signatures and Encryption، op. cit.p5

ويتحقق الركن المعنوي لهذه الجريمة في القصد الجنائي العام المتمثل في العلم والإرادة فهي جريمة عمدية لا يتصور وقوعها بطريق الخطأ[1].

وأخيراً فإن التوقيع الإلكتروني يعتبر نتيجة طبيعية للتطورات التكنولوجية الهائلة التي تشهدها المجتمعات المعاصرة في مجال المعلوماتية والاتصالات بين الأفراد والشركات، وهو بديل عن مثيله التقليدي الذي تستعمل فيه المحررات المدونة على دعامات ورقية، أو بمعنى آخر هو نتيجة للاندماج الذي تم بين المعلوماتية والاتصالات عن بعد، والذي أثمر ما يسمى المعلوماتية عن بعد[2].

وقد أصبح التوقيع الإلكتروني ظاهرة اجتماعية[3] يحميها القانون الجنائي، ويجرم الاعتداء عليه في كافة الصور باعتباره البديل عن التوقيع التقليدي، وارتباط كافة الأنشطة التجارية التي تجري عبر شبكة الإنترنت داخل الاقتصاد العالمي به، بما يستتبع قبول التوقيع في شكله الجديد وإعطاءه الحماية القانونية[4].

---

(1) د. محمد أحمد محمد نور جستنية، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، مرجع سابق، ص 39.

(2) د. محمد حسام محمود لطفي، استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامهما، القاهرة، 1993، بدون ناشر، ص 3.

(3) د. محمد السعيد رشدي: حجية وسائل الاتصال الحديثة في الإثبات، مرجع سابق، ص 49.

(4) Minyan Wang &Queen Mary, University of London، Do the regulations on electronic signatures facilitate international electronic commerce? A critical review5،computer law & s e c u r i t y r e p o r t 2 3 (2 0 0 7) 3 2، 4 1.

وقد اهتم قانون المعاملات والتجارة الإلكترونية الإماراتي بالتوقيع الإلكتروني وبتنظيمه، ولكن دون أن ينص على عقوبات خاصة به كما فعل المشرع المصري، حيث حدد في المادة (17) متى يعد التوقيع الإلكتروني محميًا بقوله:

1) يعامل التوقيع على أنه توقيع إلكتروني محمي إذا كان من الممكن التحقق من خلال تطبيق إجراءات توثيق محكمة منصوص عليها في هذا القانون أو معقولة تجاريًا ومتفق عليها بين الطرفين، من أن التوقيع الإلكتروني كان في الوقت الذي تم فيه:

أ) ينفرد به الشخص الذي استخدمه.

ب) ومن الممكن أن يثبت هوية ذلك الشخص.

ج) وأن يكون تحت سيطرته التامة سواء بالنسبة لإنشائه أو وسيلة استعماله وقت التوقيع.

د) ويرتبط بالرسالة الإلكترونية ذات الصلة به بطريقة توفر تأكيدًا يعتمد عليه حول سلامة التوقيع، بحيث إذا تم تغيير السجل الإلكتروني فإن التوقيع الإلكتروني يصبح غير محمي.

2) يعتبر الاعتماد على التوقيع الإلكتروني المحمي معقولا ما لم يثبت العكس).

كما حددت المادة (*19*) واجبات الموقع، وهي على النحو التالي:

أولا: يجب على الموقع:

1) عدم استخدام أداة توقيعه استخدامًا غير قانوني.

2) أن يمارس عناية معقولة لتفادي استخدام أداة توقيعه استخدامًا غير مصرح به.

3) أن يخطر الأشخاص المعنيين بدون تأخير غير مبرر، وذلك في حالة:

أ) معرفة الموقع بأن أداة توقيعه تعرضت لما يثير الشبهة في درجة أمانها.

ب) أو إذا تبين من دلالة الظروف المعروفة لديه ما يرجح أن أداة التوقيع قد تعرضت لما يثير الشبهة فيها.

4) أن يمارس عناية معقولة لضمان دقة واكتمال كل ما يقدمه من بيانات وتصريحات جوهرية ذات صلة بشهادة المصادقة الإلكترونية طوال مدة سريانها، وذلك في الحالات التي تستلزم فيها أداة التوقيع استخدام هذه الشهادة.

ثانيًا: يكون الموقع مسئولا عن تقصيره في استيفاء متطلبات الفقرة (أولا) من هذه المادة).

ومن القوانين العربية التي اهتمت بالتوقيع الإلكتروني منذ وقت مبكر القانون البحريني، حيث نظم التوقيع الإلكتروني وأفرد عقوبات خاصة به، فنصت المادة (6) منه والتي جاءت تحت عنوان "التوقيع الإلكتروني" على أنه:

1) لا ينكر الأثر القانوني للتوقيع الإلكتروني، من حيث صحته وإمكان العمل بموجبه، لمجرد وروده - كليًا أو جزئيًا - في شكل إلكتروني.

2) إذا أوجب القانون التوقيع على مستند، أو رتب أثرا قانونيًا على خلوه من التوقيع، فإنه إذا استعمل سجل إلكتروني في هذا الشأن، فإن التوقيع الإلكتروني عليه يفي بمتطلبات هذا القانون.

3) إذا عرض بصدد أية إجراءات قانونية توقيعَ إلكتروني مقرون بشهادة معتمدة قامت القرينة على صحة ما يأتي ما لم يثبت العكس أو يتفق الأطراف على خلاف ذلك:

أ) أن التوقيع الإلكتروني على السجل الإلكتروني هو توقيع الشخص

المسمى في الشهادة المعتمدة.

ب) أن التوقيع الإلكتروني على السجل الإلكتروني قد وضع من قبل الشخص المسمى في الشهادة المعتمدة بغرض توقيع هذا السجل الإلكتروني.

ج) أن السجل الإلكتروني لم يطرأ عليه تغيير منذ وضع التوقيع الإلكتروني عليه.

4) إذا لم يتم وضع التوقيع الإلكتروني باستعمال شهادة معتمدة، فإن قرينة الصحة المقررة بموجب أحكام البند السابق لا تلحق أيًّا من التوقيع أو السجل الإلكتروني.

وفي فصل العقوبات نص على جرائم حديثة تمثل اعتداءً على التوقيع الإلكتروني، فنصت المادة (24) منه على: (1 - مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر، يعاقب بالسجن مدة لا تزيد على عشر سنوات، وبغرامة لا تجاوز مائة ألف دينار، أو بإحدى هاتين العقوبتين كل من ارتكب عمدًا فعلا من الأفعال الآتية:

أ) نسخ أو حيازة أو إعادة تكوين أداة إنشاء توقيع إلكتروني لشخص آخر، أو الدخول على أداة إنشاء هذا التوقيع دون تفويض بذلك من هذا الشخص وبسوء نية.

ب) تحريف أو تغيير أو استعمال أو إفشاء أداة إنشاء توقيع إلكتروني لشخص آخر دون تفويض منه بذلك، أو بما يجاوز حدود هذا التفويض.

ج) إنشاء أو نشر أو تحريف أو استعمال شهادة أو توقيع إلكتروني لغرض احتيالي، أو لأي غرض غير مشروع.

د) انتحال هوية شخص آخر، أو الادعاء زورًا بأنه مفوض من قبله في

طلب الحصول على شهادة أو قبولها، أو طلب تعليق العمل بها أو إلغائها.

هـ) نشر شهادة أو وضعها في متناول أي شخص يحتمل أن يعتمد عليها أو على توقيع إلكتروني وارد بها من خلال الاستناد لأية بيانات مدرجة بهذه الشهادة، مثل الرموز أو كلمات السر أو مفاتيح التشفير العامة أو أية بيانات تستعمل لأغراض التحقق من صحة التوقيع الإلكتروني، إذا كان من ارتكب ذلك الفعل على علم بأي من الآتي:

- عدم إصدار الشهادة من قبل مزود خدمة الشهادات المدون في تلك الشهادة.
- عدم قبول الشهادة من قبل صاحبها المدون بها.
- إلغاء الشهادة أو وقف العمل بها، بشرط ألا يكون نشر الشهادة أو وضعها في متناول الجمهور قد تم بغرض تمكين الغير من التحقق من صحة توقيع إلكتروني تم إنشاؤه قبل إلغاء الشهادة أو وقف العمل بها، أو لغرض الإخطار بالإلغاء أو الوقف.

2) مع عدم الإخلال بأية عقوبة أشد ينص عليها أي قانون آخر، يعاقب بالحبس مدة لا تزيد على ثلاث سنوات، وبغرامة لا تجاوز عشرة آلاف دينار، أو بإحدى هاتين العقوبتين، كل شخص منع عمدًا أحد رجال الضبط القضائي أو المأذون بالاستعانة بهم في إجراء التفتيش، أو حال دون قيام أي منهم بالأعمال المنصوص عليها في المادة (23) من هذا القانون).

أما الدول التي لا توجد بها نصوص قانونية تنظم التوقيع الإلكتروني وتضفي عليه الحماية الجنائية فقد أخذت بانطباق النصوص التقليدية على تزوير التوقيع الإلكتروني، وقرروا أن هذا التوقيع عبارة عن مجموعة من

الإجراءات تؤدي في النهاية إلى نتيجة معينة، وهو ما يعبر عنه اختصارًا بـ (الكود أو الشفرة) أو الرمز أو الرقم، فهو ليس مكتوبًا بخط الموقع كما أوضحنا، وهو البديل الحديث عن التوقيع العادي، وإن كان من حيث الشكل يختلف عنه اختلافًا جوهريًا، ويتم غالبًا في غيبة الطرف الآخر.

وبظهور المستند الإلكتروني يعتقد البعض أن الكتابة فقدت قيمتها بعد ظهور شبكة الإنترنت، لذلك فالتلاعب في التوقيع الإلكتروني بإدخال بيانات معلوماتية كاذبة تؤدي إلى التزوير في الكود أو الرموز أو الشفرة أو الرقم تقوم به جريمة التزوير، وكذا بوضع إمضاءات أو أختام أو بصمات مزورة، أو وضع أسماء أو صور أشخاص آخرين مزورة، واعتبروا أن التقليد والاصطناع وهما من طرق التزوير المؤثمة قانونًا تقومان بجعل واقعة مزورة في صورة واقعة صحيحة، وتشمل هذه الصورة كل تقرير لواقعة على غير حقيقتها، فإذا ما تم تغيير الحقيقة بوضع إمضاء مزور فإن القانون يعاقب على وضع هذا التوقيع المزور ولا يتطلب تقليده، متى كان من شأن التوقيع بهذا الاسم أن يوهم بصدور المحرر من الشخص المزوَّر عليه[1].

فالقانون لا يشترط في الإمضاءات أن تكون عن طريق تقليد للإمضاءات الحقيقية، فيكفي التوقيع باسم صاحب الإمضاء ولو كان اسمه مخالفًا للإمضاء الحقيقي، فالتوقيع على المحرر بإمضاء مزور يعد تزويرًا معاقبًا عليه ولو كان الإمضاء لشخص لا وجود له[2].

(1) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، مرجع سابق، ص 141.
(2) د. السيد عتيق، جرائم الإنترنت، مرجع سابق، ص 127.

المبحث الثاني

جرائم إساءة استخدام بطاقات الدفع الإلكتروني

يرجع ظهور التجارة الإلكترونية وانتشارها المذهل إلى التقدم العلمي الهائل في وسائل الاتصالات وثورة المعلومات التي غزت العالم عبر شبكة الإنترنت، وانطلاقًا من هذه التسمية الخاصة بهذا النوع الحديث من التجارة يتطلب ذلك أن تكون وسائل الوفاء والدفع في تلك التجارة تتم أيضًا بطريقة إلكترونية، وذلك من خلال قنوات اتصال إلكترونية، مما يؤدي إلى سرعة تسوية المدفوعات، مما له أبلغ الأثر على التوسع في التبادل التجاري عن بعد(1).

وقد حاولت توصية اللجنة الأوروبية الصادرة في 30 يوليو 1997 وضع موجهات في شأن العمليات التي تتم عن طريق وسائل الدفع الإلكترونية، والتي تمتد لتشمل السداد بطريق شبكة الإنترنت وخصوصًا فيما يتعلق بمصدر البطاقة وحاملها، ومن هذه الموجهات اتخاذ الاحتياطيات اللازمة لتأمين المعاملات، وأكدت المبادرة الأوروبية في شأن التجارة الإلكترونية أن الاستخدام غير المشروع وتزوير بطاقات الائتمان من أهم المخاطر التي تواجه التجارة الإلكترونية، وهي أفعال لا يعاقب عليها إلا في عدد محدود من الدول(2).

وتعد بطاقات الوفاء من وسائل الدفع الحديثة التي ابتدعتها البنوك، وهي تعد مظهرًا من مظاهر التطور في الحياة التجارية بشقيها التقليدي

(1) د. محمد نور الدين سيد، المسئولية الجنائية عن الاستعمال غير المشروع لبطاقات الوفاء، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2005، ص 44.

(2) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 137.

والإلكتروني[1]، فقد كانت بدايتها في الولايات المتحدة الأمريكية في مطلع هذا القرن[2]، وتطورت فكرتها ونظامها حتى أصبح لها مكانة مهمة بين أدوات الدفع الأخرى ومنها الشيك[3]، لذا فمن الأهمية بمكان تعريفها، والتفرقة بينها وبين الشيك، حيث إن بيان ماهية بطاقة الوفاء يعد من المسائل الأولية التي يجب حسمها حتى يمكن تحديد نطاق حمايتها جنائيًا في ظل النصوص الحالية لقانون العقوبات، ومن المهم أيضًا محاولة بيان طبيعتها القانونية، وعلى ذلك فسوف نقسم هذا المبحث إلى مطلبين كما يلي:

المطلب الأول: تعريف بطاقة الوفاء.

المطلب الثاني: مضمون الحماية الجنائية الخاصة لبطاقة الوفاء.

المطلب الأول

تعريف بطاقة الوفاء

عرف المشرع الفرنسي بطاقة الوفاء وذلك في المادة الثانية من القانون رقم 91-1382 والصادر في 30 ديسمبر 1991 والخاص بتأمين الشيكات وبطاقات الوفاء، بأنها أداة تصدر من إحدى مؤسسات الائتمان أو إحدى الجهات المنصوص عليها في المادة (8) من القانون رقم 84-46 والصادر في 24 يناير 1984 والخاص بنشاط ورقابة مؤسسات الائتمان،

(1) Angel J:why use Digital signatures for Electronic commerce? Commentary 1999، the journal of information،Law and Technology (JIL T)، p4
"http://eli.warwick.ac.uk\Jilt\199،2\angel.html"

(2) GAVALDA (C.), Les cartes de paiement et de credit, DALLOZ, 1994, p. 1.

(3) (MARTIN (Didier R.), la carte de paiement et la loi Ou la puce maltraitee), D. S. H., octobre 1992, ch. P. 277.

وتسمح لحاملها بسحب أو تحويل نقود من حسابه.

ويرى البعض أن هـذا التعريـف الشـكلي لبطاقـة الوفـاء والـذي يعتمـد عـلى الجهــة التـي أصدرت البطاقة قد لا يكفي لتحديد المقصود بها وتمييزها عـن غيرها.

فبطاقة الوفاء هي تلك الأداة التي تسمح لحاملها باتخاذ الإجراءات اللازمة والمباشرة لخصم المبلغ الذي يحدده لمصلحة شـخص آخر مـن حسابه لـدى البنك الـذي أصـدر هــذه البطاقـة[1]، ومؤدى ذلك أن بطاقة الوفاء تفترض وجـود ثلاثة أشخاص: حامل البطاقة، البنك مصـدر البطاقـة والذي يوجد به حساب حاملها، والمستفيد أو الدائن لهذا الأخير[2].

وعرفها القضاء بأنها مستند يعطيه مصدره لشخص طبيعي أو اعتباري بناءً على عقد بيـنهما يمكنه من شراء السلع والخـدمات ممـن يعتمـد المسـتند دون دفـع الـثمن حـالا لتضـمنه التـزام المصدر بالدفع، ومنها ما يمكّن من سحب النقـود مـن المصـارف، وتكـون علاقـة المصرف مصـدر بطاقة الائتمان بعميله المسلمة له البطاقة علاقة عقد انضمام، يلتزم بمقتضاه العميـل باسـتخدام البطاقة بحسن نية وبالمحافظة عليها وعلى الـرقم السري الخـاص بهـا، فـإذا ضـاعت البطاقـة أو سرقت منه فعليه أن يسارع بإخطار المصرف (مصدرها) بفقدانها أو سرقتهـا، فـإن لم يفعـل ذلـك وتم التعامل بها قبل إخطار العميل المصرف بضياعها أو سرقتها يلتزم العميل بقيمـة مـا تـم مـن معاملات

(1) MARTIN (Didier R.).), la carte de paiement et la loi Ou la puce maltraitee), art. Prec. op. cit. P. 278.

(2) د. عمر سالم، الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية، 1995، ص 11.

- ولكن هذا لا يمنع من أن تستخدم بطاقة الوفاء كبطاقة سحب، وفي هذه الحالة يفـترض تـوافر شخصـين: البنك وحامل البطاقة.

ما دام لم يقع إهمال من التاجر المتعامل معه في الإجراءات المعتادة[1].

وتعد بطاقة الوفاء وفقًا للتحديد السابق أداة وفاء بطبيعتها، شأنها في ذلك شأن الشيك، فإذا كان هذا الأخير يستوجب الدفع بمجرد الاطلاع، ولا يجوز الرجوع فيه إلا في حالات محددة على سبيل الحصر، فإن بطاقة الوفاء كذلك، إذ بمجرد إصدار أمر الدفع سواء بالتوقيع اليدوي أو بالوسائل الأوتوماتيكية كإدخال الرقم السري في الجهاز المعد لذلك فإنه لا يجوز الرجوع فيه إلا في حالات محددة[2] كحالة فقد الكارت أو سرقته.

وإذا كانت بطاقة الوفاء تعد أداة وفاء تتم بطريقة إلكترونية ولا فارق بينها وبين الشيك إلا فيما يتعلق بطريقة أدائها لعملها، فهل يمكن أن تطبق عليها ذات القواعد الخاصة بالشيك؟ وتُقرر مساءلة حاملها عن جريمة إصدار شيك بغير رصيد إن توافرت أركانها.

الحقيقة أنه على الرغم من أن للشيك في القانون الجنائي مدلولا مستقلا عنه في القانون التجاري[3]، إلا أنه من الصعب اعتبار بطاقة الوفاء شيكًا وخضوعها بالتالي لنفس أحكامه، فالشيك وبطاقة الوفاء يمثلان وسيلتين مختلفتين للوفاء، ويثيران في العمل مشكلات قانونية مختلفة، وذلك

(1) حكم محكمة تمييز دبي بتاريخ 4 / 6 / 2005 في الطعن رقم 2005/121 طعن تجاري.

(2) GREDOT (F. J.) Conditions et effets des oppositions en matiere de carte de paiement, petites Affiches l986, no 22, p. 105.

(3) د. محمود محمود مصطفى، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 570, وفي المعنى ذاته: د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، ص 1066، د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، مرجع سابق، ص 938 , وفي المعنى ذاته: د. عبد العظيم مرسي وزير، شرح قانون العقوبات، القسم الخاص، جرائم الاعتداء على الأموال , دار النهضة العربية، 1993، ص 449.

على النحو الذي سنراه بعد قليل، ومما يؤكد هذا الاختلاف بين الوسيلتين أن المشرع الفرنسي قد أصدر قانونًا جديدًا أسماه "أمن الشيكات وبطاقات الوفاء"[1].

وفي كل الأحوال فإن مبدأ الشرعية يأبى قياس بطاقة الوفاء على الشيك وامتداد حمايته الجنائية إليها، لذا يجب البحث في النصوص الجنائية الحالية لمعرفة ما يمكن أن تكفله من حماية جنائية لها وهو ما سنبحثه في المطلب التالي.

المطلب الثاني

مضمون الحماية الجنائية الخاصة لبطاقة الوفاء

القانون الإماراتي ومثله المصري لم يتضمن نصوصًا خاصة ببطاقات الائتمان، وبالتالي فإن المرجع في ذلك للقواعد العامة الواردة في قانون العقوبات سواء باعتبارها مالا أو محررًا.

فالقانون يسبغ حمايته على بطاقة الوفاء من تزويرها، وذلك في الأحكام العامة في جريمة التزوير في المحررات فتطبق على حالة تزوير بطاقة الوفاء سواء انصب التزوير على الحروف المطبوعة أو المعالجات الإلكترونية الخاصة بهذه البطاقات.

والاستعمال غير المشروع لبطاقة الوفاء من قبل الغير يكون إما باستعمال بطاقة وفاء مزورة وينسب إلى من قام بذلك جريمة استعمال المحرر المزور إذا قام باستعماله فعلا، أو بسرقة بطاقة الائتمان فتقوم جريمة السرقة باختلاس بطاقة الوفاء، واتجاه نية المتهم لتملكها أو مجرد

---

(1) Mohan Atreya and Benjamin Hammond and Stephen Paine and paul starret and Stephen Wu: Digital signatures، McGraw ،Hill\Osborn Op. Cit,،P5

الاحتفاظ بها وحرمان حاملها من استعمالها، وكذلك تقوم إذا استولى عليها بنية استعمالها وإعادتها لصاحبها[1].

(1) انتشرت في السنوات الأخيرة جرائم سرقة بطاقات الائتمان، وهناك طريقتان رئيسيتان منتشرتان لارتكاب جرائم الاحتيال على البطاقات الائتمانية، أولهما إمكانية سرقة بطاقات الائتمان واستخدامها المحتمل، ومن السهل السيطرة على هذه الطريقة من خلال إخطار البنك مباشرة بسرقة البطاقة، أما الطريقة الثانية وهي الدخول إلى الحساب فهذه الطريقة تتطلب استخدام تقنيات بدون وجود البطاقة (أي الطلب من خلال الهاتف أو شبكة الإنترنت)، أو بوجود البطاقة وتمريرها عبر ماسح ضوئي خاص (نسخ البطاقة) والاستحواذ على الحساب (أي معرفة البيانات الشخصية وانتحال الشخصية)، ويكون ذلك من خلال الإفصاح عن البيانات الشخصية مثل معلومات البطاقة البنكية أو البطاقة الائتمانية.
وبالنسبة لعدد القضايا التي تابعتها إدارة المباحث الإلكترونية في شرطة دبي خلال عام 2008 فقد بلغ 222 قضية بواقع 87 قضية احتيال وجرائم مالية و38 جريمة اختراق شبكات و92 قضية تشهير وابتزاز وخمس قضايا لمواقع وهمية قصد بها الاحتيال على المتعاملين، فيما سجلت إدارة الأدلة الإلكترونية (إحدى الإدارات الفرعية بالإدارة العامة للأدلة الجنائية) 330 قضية في 2008 شملت فحص عدد كبير من الأجهزة يصل إلى نحو 6000 جهاز.
وتعد من أهم القضايا التي تم ضبطها عصابة نيجيرية متخصصة في اختراق الحسابات البنكية وتزوير البطاقات الائتمانية, كما تم ضبط عصابة أخرى تخصصت في الإيقاع بضحاياها عبر استغلالهم في استخدام بطاقات الائتمان المزورة في عمليات سحب وشراء من المراكز التجارية مقابل نسبة خمسين في المائة, وهذه المجموعة اتخذت أسلوبًا جديدًا في نطاق جرائم بطاقات الائتمان، بالبحث عن شركاء يتولون عمليات السحب والشراء، بينما يتوارى أفراد العصابة بعيدًا عن الأنظار مقابل نسبة مئوية من حصيلة الاستخدام.
كما تمكنت أجهزة البحث الجنائي بشرطة الشارقة من الإيقاع بعصابة جديدة تضم ثلاثة أشخاص من جنسية أسيوية وبحوزتهم 31 بطاقة ائتمان صادرة من عدد من البنوك المحلية والأجنبية العاملة في الإمارات، وبالتحقيق مع أفراد العصابة=

والاستعمال غير المشروع لبطاقة الوفاء من قبل حاملها يتحقق بالتعسف في استخدامها، كأن يتم استخدامها على الرغم من انتهاء صلاحيتها، ونستطيع تحديد صور هذا الاستعمال على النحو التالي:

أولا: استخدام بطاقة الوفاء رغم عدم وجود رصيد، ويكون ذلك بأحد وجهين:

1) إما بالسحب من جهاز توزيع العملة على الرغم من عدم وجود رصيد وقت السحب، وفي هذه الحالة لا يمكن اعتبار تصرف العميل في استخدام البطاقة التي يحملها جريمة، وإنما هو مخالفة لشروط التعاقد المبرم بين البنك والعميل، ولا يدخل تحت نصوص قانون العقوبات.

2) ويكون الاستعمال غير المشروع أيضًا باستخدام البطاقة لدى أحد

= المذكورة تبين أنهم يقومون باستصدار تأشيرات زيارة عن طريق شركة يملكونها في إحدى المناطق الحرة بالدولة بهدف جلب أشخاص للدولة على أنهم مدراء ويتقاضون رواتب عالية، ثم يقومون بفتح حسابات بأسماء هؤلاء الأشخاص لدى البنوك، ويقومون بتزوير كشوفات حسابات بأسمائهم وتقديمها للبنوك لطلب إصدار بطاقات ائتمان ودفاتر شيكات.

كما يقومون باستخراج بطاقات هواتف بأسماء هؤلاء الموظفين، وبعد الحصول على بطاقات الائتمان من البنوك يقوم المذكورون بتسفير الأشخاص الذين تمكنوا من جلبهم إلى الدولة، واستخدام البطاقات في سحب الأموال من البنوك، وعندما تتقدم البنوك ببلاغات بعدم السداد تكتشف أن أصحاب هذه البطاقات غير موجودين في الدولة، وبذلك يتمكن أفراد العصابة من الحصول على مبالغ مالية كبيرة عن طريق بطاقات ائتمان صحيحة ولكن أصحابها غير موجودين في الدولة.

http://www.uaeec.com/news-action-show-id-18787.htm
http://www.ict.gov.qa/output/NewsPage.aspx?PageID=868
http://www.alkhaleej.ae/portal/84ce079b-52fa-4285-8c1a-60ac348633ad.aspx
http://www.arabianbusiness.com/arabic/552868

التجار للوفاء بثمن سلعة أو خدمة على الرغم من عدم وجود رصيد، ويطبق عليه الحكم السابق ذاته.

ثانيًا: قيام حامل البطاقة باستخدامها على الرغم من انتهاء صلاحيتها أو إلغائها، ويتحقق ذلك بأحد وجهين:

1) استخدام البطاقة على الرغم من انتهاء صلاحيتها، وفي هذه الحالة لا تقوم جريمة النصب إلا إذا كان حامل البطاقة لا ينوي تجديدها مرة أخرى، أو كان قد أغلق حسابه لدى البنك، أما في غير هذه الحالات فقد جرى العمل على قيام البنك بإعطاء بطاقة جديدة للعميل بمجرد انتهاء صلاحية الأولى مما ينتفي معه القصد الجنائي لديه.

2) استخدام البطاقة على الرغم من إلغائها، فلا يعد حامل البطاقة مرتكبًا لجريمة خيانة أمانة إلا إذا طالبه البنك برد البطاقة بسبب تعسفه في استعمالها، واستمراره في استعمالها على الرغم من ذلك.

وقد نص المشرع الفرنسي على الحماية الخاصة لبطاقة الوفاء في المادة الحادية عشرة من قانون 91-1882 والتي عدلت المادة (67) من المرسوم بقانون 30 أكتوبر 1935، إذ تنص هذه المادة على إدخال المادتين 1/67، 2/67 بعد المادة 67 من هذا القانون الأخير.

وقد نص في المادة 1/67 على أن يعاقب بالعقوبات المنصوص عليها في المادة (67)[1] (بالحبس من عام إلى سبعة أعوام، والغرامة من 3.600 فرانك حتى 500.000 فرنك، أو إحدى هاتين العقوبتين

(1) النص الفرنسي للمادة (67):

((seront punis d un emprisonne d' un an á sept ans et d' une amende de 3 600 F a 500000 F ou de l une de ces deux peines seulement...))

فقط)[1]:

1) كل من قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب.

2) كل من استعمل أو حاول استعمال البطاقة المقلدة أو المزورة وهو عالم بذلك.

3) كل من قبل الدفع ببطاقة الوفاء على الرغم من علمه بتقليد البطاقة أو تزويرها.

ووفقا للمادة 2/67 فإنه في الحالات السابقة يتعين مصادرة وتدمير الشيكات والبطاقات المقلدة أو المزيفة، وكذلك مصادرة المواد والماكينات والمعدات أو الأدوات التي استخدمت أو التي كانت متجهة إلى الاستخدام في التزييف أو التقليد، إلا إذا استخدمت بدون علم المالك[2].

ونفصل صور هذه الحماية الجنائية الخاصة، ثم نبين مدى كفايتها، وقد عاقب التشريع الفرنسي في هذا الشأن على ثلاث جرائم، سوف نتناولها، كما نتناول العقوبات المقررة لها وفقًا لورودها في القانون الفرنسي، وذلك

---

(1) نص المادة (67 /1):

((seront punis des péines prevues a l article 67:

1) Ceux qui auront contrefait ou falsifie une carte de paiement ou de retrait;

2) Ceux qui en connaissance de cause auront fait usage ou tente de faire usage d' une carte de paiement ou de retrait contrefaite ou falsifiee;

3) Ceux quien connaissance de cause, auront accepte' de recevoir un paiement au moyen d une carte de paiement contrefaite ou falsifiee.)).

(2) ((Dans les cas prévus par les articles 67 et 67.1, les cheques et les cartes de paiement ou de retait contrefaits ou falsifies seront confisqués et detruits. La confiscation, des matiéres, machines, appareils ou instruments qui ont servi ou etait destines á servir á la fabrication desdits objets sera prononceé, sauf lorsqu il s ont eté utilisees á l insu du proprietaire)).

في أربعة فروع: الأول في جريمة تقليد أو تزوير بطاقة الوفاء، والثاني في جريمة استعمال أو محاولة استعمال البطاقة المزورة أو المقلدة، والثالث جريمة قبول التعامل بالبطاقة على الرغم من العلم بتزويرها أو تقليدها، وحيث إن المشرع قد حدد لكل هذه الجرائم عقوبة أصلية وأخرى تبعية فإننا سوف نتبع هذه الفروع بفرع رابع حول العقوبات الجنائية المقررة لها، وذلك كله على النحو التالي:

الفرع الأول

جريمة تقليد أو تزوير بطاقة الوفاء

تتمثل أركان هذه الجريمة في نص المادة (1/67) من القانون سالف البيان: " كل من قام بتقليد أو تزوير بطاقة وفاء أو سحب". وعلى الرغم من أن المشرع لم يوضح في هذا النص كافة الأركان التي تقوم عليها هذه الجريمة، إلا أنه استنادًا إلى القواعد العامة في التزوير عمومًا، وخاصة نص المادة 1/441 من قانون العقوبات الفرنسي الجديد، يمكن أن نقيم بنيان هذه الجريمة على الأركان الأربعة الآتية: موضوع ينصب عليه نشاط الجاني يتمثل في بطاقة الوفاء أو السحب، وركن مادي، وضرر، وركن معنوي، ونبحث تباعًا هذه الأركان فيما يلي:

أولا: الموضوع الذي ينصب عليه نشاط الجاني:

حدد المشرع الفرنسي موضوع هذه الجريمة بقوله: " بطاقة الوفاء أو السحب[1] " وفقا للتعريف الوارد في المادة 1/57 من قانون 30 أكتوبر 1935 والمعدلة بقانون 30 ديسمبر 1991 بقوله: " تعد بطاقة وفاء كل بطاقة صادرة من مؤسسة ائتمان أو هيئة أو مرفق مما نص عليه في المادة

(1) يلاحظ أن بطاقة الوفاء دائمًا ما تستخدم كبطاقة سحب.

(8) من قانون رقم 46/84 والصادر في 24 يناير 1984 الخاص بنشاط ورقابة مؤسسات الائتمان، وتسمح لحاملها بسحب النقود أو تحويلها "[1]، ومؤدى ذلك أن الأنواع الأخرى للبطاقات كبطاقة الاعتماد أو البطاقات الخاصة[2] لا تصلح أن تكون موضوعًا لجريمة التزوير التي نص عليها المشرع في هذه المادة، وإن كان يمكن أن تخضع للنصوص العامة في التزوير في المحررات.

وعلى الرغم من ذلك فيجب ألا نغفل من ناحية أولى ذاتية القانون الجنائي، وما قد يترتب عليه من إعطاء مفهوم لبطاقة الوفاء أكثر اتساعًا من المفهوم الذي تبناه القانون التجاري، وذلك على غرار ما حدث بالنسبة لمفهوم الشيك[3]، ومن ناحية ثانية فإن البطاقة ذاتها ووفقًا للاتفاق المبرم بين العميل والجهة المصدرة لها قد تمارس وظيفة الائتمان والوفاء والسحب، مما يجعلها تدخل في نطاق التحديد التشريعي السابق، فالمشرع يريد كفالة الثقة في هذه الأداة من أدوات الوفاء بعدما ثبت أنها تؤدي وظيفة الوفاء فقرر حمايتها جنائيًا، مثلها في ذلك مثل الشيك الذي يعد أداة وفاء حسب الأصل، ولكنه يستخدم في بعض الأحيان من الناحية العملية كأداة ائتمان، ولم يمنع ذلك من حمايته جنائيًا.

---

(1) وقد عرف المشرع الفرنسي بطاقة السحب في المادة 2/57 من القانون ذاته، وهي تصدر من ذات جهات إصدار بطاقة الوفاء، ولكن يقتصر دورها على سحب النقود فقط من أجهزة التوزيع الآلي.

(2) Mohan Atreya and Benjamin Hammond and Stephen Paine and paul starret and Stephen Wu: Digital signatures ،McGraw ،Hill\Osborne OP. CIT،P14.

(3) (CHAPUT (Y.), la loi no 91،1382 du 30 decembre 1991 relative a la securite des cheques et des cartes de paiement; D. S. 1992, p. 108.

ثانيًا: الركن المادي لهذه الجريمة:

الركن المادي لجريمة تقليد أو تزوير بطاقات الوفاء يتخذ إحدى صورتين: التقليد أو التزوير[1]، وسوف نتناول كلا منهما تباعًا:

أ) **التقليد:** يقصد به عمومًا صناعة شيء على غرار شيء آخر[2]، ويقصد في مجال بطاقة الوفاء صناعة بطاقة وفاء على غرار بطاقة أخرى، ويبدو أن السبب الذي دفع المشرع إلى النص على التقليد بالذات أنه الوسيلة الوحيدة التي تحقق غرض المتهم في استعمال البطاقة بعد ذلك، فاستخدام البطاقة المقلدة يستلزم معرفة الرقم السري الخاص بها. ولكن ليس هناك ما يمنع من اصطناع بطاقة وفاء جديدة دون أن تكون على غرار بطاقة أخرى، وفي هذه الحالة يدخل الاصطناع تحت مدلول التزوير.

ب) **التزوير:** جاء لفظ التزوير عامًّا دون تحديد طرق خاصة به[3]، بما مفاده أن أي تغيير في بطاقة الوفاء ذاتها سواء بتغيير بعض أرقامها، أو الإمضاء الموقع عليها، أو الاسم المدون فوق ظهرها، أو التعديل فيما تتضمنه من معطيات إلكترونية، أو أية طريقة من طرق التزوير

---

(1) غني عن البيان أن التقليد طريق من طرق التزوير, وقد يفسر منهج المشرع بالرغبة في الفصل بين التزوير الذي يقع في البطاقة ذاتها كمحرر, والتزوير الذي يأخذ صور اصطناع بطاقة على غرار بطاقة أخرى.

(2) د. محمود نجيب حسني, شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 238.

(3) وهذا المنهج يخالف منهج المشرع الفرنسي في قانون العقوبات القديم وقانون العقوبات الحالي, إذ حدد طرق التزوير على سبيل الحصر, ويتفق مع منهج المشرع الفرنسي في قانون العقوبات الجديد حيث لم يحدد طرقا معينة للتزوير.

المادي فإن الركن المادي لهذه الجريمة يتحقق بذلك[1].

وبالنسبة للتزوير المعنوي لبطاقة الوفاء، فالثابت صعوبة وقوع ذلك نظرًا لأن بطاقة الوفاء تصدر من إحدى المؤسسات المالية، ويتبعها رقم سري معين، وتفترض وجود حساب خاص بالعميل الذي سيحمل هذه البطاقة، فإذا انتحل شخص شخصية صاحب حساب في أحد البنوك وهو يعلم أن هذا الأخير لم يحصل على بطاقة وفاء من البنك، ثم قام بطلب هذه البطاقة فصدرت بالطبع باسم صاحب الحساب الحقيقي، وقام المتهم بالحصول عليها، في هذه الحالة نكون بصدد تزوير معنوي اتخذ صورة جعل واقعة مزورة في صورة واقعة صحيحة، وذلك بانتحال شخصية الغير[2].

ثالثًا: الضرر:

على الرغم من أن المشرع لم يذكر الضرر باعتباره أحد الأركان اللازمة لقيام جريمة تزوير بطاقة الوفاء، إلا أن المستقر عليه فقهًا وقضاءً ضرورة توافر هذا الركن، ويكفي بطبيعة الحال أن يكون هذا الضرر احتماليًا.

ويتخذ الضرر في جريمة التزوير مدلولا واسعًا؛ إذ قد يكون ماديًا أو معنويًا، وقد يكون فرديًا أو اجتماعيًا، وقد يكون حالا أو احتماليًا، وغني عن البيان أن تغيير الحقيقة في بطاقة الوفاء ينطوي على ضرر احتمالي، إذ يمكن استخدامها على نحو يحقق ضررًا للأفراد أو للمؤسسات المالية، بل

(1) د. محمود محمود مصطفى، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 145, وفي المعنى ذاته: د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 230.

(2) د. عمر السعيد رمضان، قانون العقوبات، القسم الخاص، مرجع سابق، ص 157.

إن تزوير بطاقة صحيحة بنية استعمالها فيما زورت من أجله قد ينطوي على ضرر مادي حالٍّ هو إمكانية إتلاف هذه البطاقة مع ما ينطوي عليه ذلك من ضرر فعلي للبنك الذي أصدرها[1].

رابعًا: الركن المعنوي:

يتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام بشقيه العلم والإرادة، بأن يعلم الجاني أن ما يرتكبه هو فعل مجرم قانونًا، ومع ذلك فهو يتجه بإرادته لتنفيذ هذه النتيجة، وإلى جانب هذا القصد يلزم لتوافر الركن المعنوي لهذه الجريمة توافر القصد الخاص، أي يجب إلى جانب توافر القصد الجنائي العام ثبوت أن نية الجاني قد اتجهت إلى استعمال بطاقة الوفاء المزورة فيما زورت من أجله، وإضافة المتحصل منها إلى ممتلكاته.

وقد عرفت محكمة النقض المصرية القصد الجنائي في التزوير بأنه (تعمد تغيير الحقيقة في محرر تغييرًا من شأنه أن يسبب ضررًا وبنية استعمال المحرر فيما غيرت من أجله الحقيقة)[2].

كما قضت بأن القصد الجنائي في التزوير ينحصر في أمرين: الأول هو علم الجاني بأنه يرتكب الجريمة بجميع عناصرها التي تتكون منها طبقًا للقانون، أي إدراكه أنه يغير الحقيقة في محرر بإحدى الطرق المنصوص عليها قانونًا، وأن من شأن هذا التغيير أن يترتب عليه ضرر، والثاني وهو خاص بجريمة التزوير: اقتران هذا العلم بنية استعمال المحرر فيما زور من أجله[3].

---

(1) د. عمر سالم، الحماية الجنائية لبطاقة الوفاء، مرجع سابق، ص 35.
(2) نقض 16 مايو 1977 , س 28 , رقم 129 , ص 609 , مجموعة أحكام النقض.
(3) نقض 13 مارس 1944 , مجموعة القواعد القانونية, ج 6, رقم 318 , =

الفرع الثاني

جريمة استعمال أو محاولة استعمال بطاقة مقلدة أو مزورة

نص المشرع على هذه الجريمة في المادة (2/67) من القانون الفرنسي والتي جاء في نصها: "كل من استعمل أو حاول استعمال بطاقة وفاء أو سحب مقلدة أو مزورة وهو يعلم بذلك".

فهي بذلك جريمة استعمال عادية للمحررات المزورة، وإن كانت تتميز بموضوعها في أن المشرع نص صراحة على عقاب الشروع فيها، ومن الواضح أن المشرع قد فصل بين تزوير البطاقة أو تقليدها وبين استعمالها، وهذا يعني أن مرتكب جريمة التزوير يسأل عنها ولو لم يستعمل البطاقة، ومن يستعمل البطاقة المزورة يسأل عن جريمة الاستعمال ولو لم يقم بالتزوير أو يشترك فيه[1]، وسوف ندرس أركان هذه الجريمة، ثم نبحث الشروع فيها، وفي النهاية نحدد طبيعتها، وتقوم هذه الجريمة على ثلاثة أركان: موضوع ينصبُّ عليه نشاط الجاني، وركن مادي، وآخر معنوي، ونبحث ذلك تباعًا فيما يلي:

أولا: الموضوع الذي ينصب عليه نشاط الجاني:

يتمثل هذا الموضوع في بطاقة وفاء مقلدة أو مزورة، ومؤدى ذلك أن هذا الركن لا يتوافر إذا كانت البطاقة صحيحة وقام شخص باستعمالها، إذ

= ص 430، مشار إليه لدى د.عمر سالم، الحماية الجنائية لبطاقات الوفاء، مرجع سابق، ص 30.

(1) د. محمود محمود مصطفى، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 178، ويرى أن المتهم إذا ارتكب الجريمتين يسأل عنهما وتطبق عليه إحدى العقوبتين فقط وفقا لقواعد الارتباط.

إنه يسأل في هذه الحالة عن جريمة نصب عند البعض[1]، وجريمة سرقة عند البعض الآخر[2]، بيد أنه من الملاحظ أن اشتراط توافر جريمة تزوير البطاقة أو تقليدها لا يعني ضرورة توافر الركن المعنوي لدى المزور أو المقلد؛ إذ قد تقوم جريمة الاستعمال إذا قام شخص بتزوير بطاقة أو تقليدها ابتغاء إظهار مهارته، ثم تصل إلى حوزة آخر فيقوم باستعمالها[3]، فبراءة المزور بسبب انتفاء الركن المعنوي لا تقود إلى براءة من استعملها، ويعد ذلك نتيجة طبيعية للفصل بين جريمة التزوير والاستعمال[4].

ثانيا: الركن المادي:

يتمثل الركن المادي في جريمة استعمال المحرر المزور في فعل

---

(1) وفقا للقضاء الفرنسي يعد مرتكبا لجريمة نصب من يحاول الحصول على نقود عن طريق إدخال كارت ليس له في إحدى آلات توزيع الأوراق النقدية مما يجعله مرتكبا لجريمة النصب حتى ولو لم ينجح في ذلك، كما طبقت محكمة النقض الفرنسية التكييف ذاته على استخدام وسائل احتيالية عند شراء بضاعة من أحد التجار وسداد ثمنها عن طريق بطاقة ائتمان مسروقة، مستعملا في ذلك اسم حامل البطاقة المدون عليها، وقيامه بالتوقيع بهذا الاسم على فاتورة البضاعة التي قدمها التاجر.

- د. عمر سالم، الحماية الجنائية لبطاقات الوفاء، مرجع سابق، ص 41.

(2) د. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، مرجع سابق، ص 134.

(3) وغني عن البيان أنه يتعين ثبوت أن تزوير البطاقة قد يؤدي إلى حدوث ضرر بالغير، ومؤدى ذلك أنه إذا ثبت أن التزوير كان مفضوحًا بحيث لا يمكن استعمالها، فإن جريمة الاستعمال ذاتها تنتفي.

(4) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، مرجع سابق، ص 312.

الاستعمال، أي إحراز المحرر والاحتجاج به على أنه صحيح[1]، وإذا طبقنا ذلك على بطاقة الوفاء فإننا نعني به إحراز البطاقة والاحتجاج بها على أنها صحيحة، ومؤدى ذلك أن مجرد وجود البطاقة المزورة في حيازة المتهم دون إحرازها لا يقوم به فعل الاستعمال، فيتعين أن يقوم المتهم بإحراز البطاقة والاحتجاج بها على أنها صحيحة، ويكون ذلك عندما يستخدمها في الوفاء لدى أحد التجار، ويترتب على ذلك أنه إذا قدم المتهم البطاقة إلى هذا الأخير وأخبره أنها ليست صحيحة، وعلى الرغم من ذلك قبل التاجر الوفاء بها، ففي هذه الحالة يرتكب التاجر جريمة قبول التعامل ببطاقة الوفاء على الرغم من العلم بتزويرها أو تقليدها، ويعتبر حامل البطاقة شريكًا في هذه الجريمة.

وإذا كان جوهر الاستعمال يتمثل في إحراز البطاقة المزورة والاحتجاج بها فإنه يتعين أن يكون إراديًا، ومؤدى ذلك أن مجرد ضبط البطاقة مع المتهم وثبوت تزويرها وادعاؤه أنها صحيحة لا يجعله مرتكبًا لجريمة الاستعمال.

واستعمال بطاقة الوفاء المزورة يتحقق بطبيعة الحال عندما يقوم المتهم بتقديمها لأحد التجار على أنها بطاقة صحيحة، ولكن هل يتحقق الاستعمال كذلك في حالة قيامه باستخدامها في السحب من إحدى آلات التوزيع الآلي؟

على الرغم من أن تعبير الاحتجاج بها على أنها بطاقة صحيحة قد يكون غريبًا في حالة السحب من الآلة، إلا أن المشرع قد ذكر تعبير " من استعمل " والاستعمال يتحقق سواء بالوفاء بها لدى أحد التجار أو عند

(1) د. عمر السعيد رمضان، قانون العقوبات، القسم الخاص، مرجع سابق، ص 202.

استخدامها في السحب من الآلة[1]، ومما يؤكد ذلك أن المشرع قد جرم مجرد المحاولة وأعطاها حكم الجريمة الكاملة، وتبدو أهمية المحاولة عند استعمال البطاقة المزورة في السحب من الجهاز الآلي[2].

ثالثًا: الركن المعنوي:

يتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي العام، أي العلم بتزوير البطاقة أو تقليدها، وإرادة إبرازها والاحتجاج بها على أنها بطاقة صحيحة، فينتفي هذا القصد إذا ثبت أن مستعملها لا يعلم بتزويرها[3]، فجريمة استعمال المحرر المزور تنتفي بصفة عامة إذا ثبت جهل المتهم بتزوير المحرر، وينتفي القصد الجنائي كذلك إذا لم تتجه إرادة المتهم إلى استعمال البطاقة، وإنما ضبطت معه فادعى صحتها.

---

(1) GAVALDA (C.), le droit penal des cartes de paiement et \ ou credits, oP. cit; p. 92.

(2) قضي بأن المسئولية عن قيمة البضاعة والخدمات التي يتم الحصول عليها بمقتضى بطاقات الائتمان المزورة أو المقلدة تقع تبعتها على من تسبب بخطئه في إتمام المعاملة بموجبها من أي من طرفي العلاقة التعاقدية، وهي الجهة مصدرة البطاقة والتاجر الذي تعاقد معها على التعامل بها، ومتى كان جهاز الصرف المسلّم للتاجر من الشركة المتعاقد معها قد قبل التعامل بموجب البطاقة المقدمة للتاجر فإن عبء إثبات خطئه فيما تدعيه الشركة من أنه لم يتحقق من صحة هذه البطاقة يقع على عاتقها، فإذا لم يثبت الخطأ في جانب التاجر فإن تحمل تبعة المسئولية عن التصرف تقع على عاتق الجهة المذكورة.
حكم محكمة تمييز دبي بتاريخ 20 / 4 / 2003 في الطعن رقم 2003/14 طعن حقوق.

(3) يصعب تحقق ذلك في العمل حتى ولو كان مستعمل البطاقة شخصًا آخر غير من زورها.

رابعا: الشروع في الاستعمال:

عبر المشرع عن الشروع في هذه الجريمة بقوله: "من حاول استعمالها" ويتحقق ذلك عندما يفشل المتهم في تحقيق النتيجة الإجرامية المترتبة على هذا الاستعمال، وهي الحصول على الخدمة أو السلعة عندما يستخدمها كوسيلة للوفاء، أو الحصول على النقود إذا استخدامها كوسيلة للسحب، والحقيقة أن التفرقة بين الاستعمال ومحاولة الاستعمال تبدو قليلة الأهمية، فالمشرع قد ساوى في العقاب بين الجريمة التامة ومجرد المحاولة.

خامسًا: طبيعة جريمة استعمال بطاقة الوفاء المزورة أو المقلدة:

لتحديد طبيعة الجريمة الماثلة وما إذا كانت جريمة استعمال بطاقة الوفاء المزورة مستمرة أم وقتية، نستطيع القول بأنه يصعب اعتبار جريمة استعمال البطاقة المزورة من الجرائم المستمرة، ذلك أن الضابط في اعتبار الجريمة وقتية أو مستمرة هو الوقت الذي يستغرقه تحقق كافة عناصرها، فإذا كان ذلك يستغرق لحظة بسيطة من الزمن اعتبرت الجريمة وقتية، وإذا احتاج تحقق هذه العناصر إلى وقت طويل نسبيًا فإن الجريمة تكون مستمرة[1]، وإذا طبقنا ذلك على استعمال بطاقة الوفاء تبين لنا أنها جريمة وقتية؛ إذ إن تقديم البطاقة كوسيلة وفاء أو وسيلة للسحب من آلات توزيع النقود لا يستغرق إلا برهة قليلة من الزمن.

واعتبارها من الجرائم الوقتية يعني أنها تتجدد بتجدد الاستعمال، بمعنى أن هذه الجريمة تتحقق بكافة عناصرها في كل مرة يتم فيها استعمال البطاقة كوسيلة وفاء أو كأداة للسحب[2].

(1) د. محمود نجيب حسني، شرح قانون العقوبات، القسم العام، مرجع سابق، ص316.
(2) د. محمود محمود مصطفى، قانون العقوبات، القسم الخاص، مرجع سابق، ص182.

الفرع الثالث

جريمة قبول التعامل ببطاقة مقلدة أو مزورة

نص المشرع على هذه الجريمة في المادة (3/67) من القانون الفرنسي، حيث جاء فيها: "كل من قبل الدفع عن طريق بطاقة وفاء مقلدة أو مزورة وهو يعلم بذلك"، ويواجه المشرع بهذه الجريمة حالة استخدام البطاقة كوسيلة وفاء فقط، بحيث يسأل التاجر أو صاحب الخدمة الذي يقبلها على الرغم من علمه بتزويرها، وتقوم هذه الجريمة على ثلاثة أركان، ركن الموضوع وينصبُّ عليه نشاط المتهم، وركن مادي، وآخر معنوي.

أولا: الموضوع الذي ينصب عليه نشاط المتهم:

يتمثل الموضوع الذي ينصب عليه نشاط المتهم في النشاط الإجرامي للجاني في بطاقة وفاء مقلدة أو مزورة.

ثانيًا: الركن المادي:

يتمثل الركن المادي في هذه الجريمة في قيام شخص بقبول الوفاء عن طريق البطاقة على الرغم من علمه بتقليدها أو تزويرها، ويكون هذا الشخص في العادة تاجرًا أو شخصًا آخر يقوم بأداء خدمة معينة، ويثور التساؤل حول تحديد جدوى هذا النص، وبتعبير آخر: ألم تكن القواعد العامة في المساهمة الجنائية تؤدي إلى النتيجة نفسها؟

قبل الإجابة على هذا السؤال يتعين التنويه إلى أن المجني عليه في هذه الحالة لن يكون التاجر، وإنما البنك المسحوب عليه، وربما صاحب الحساب الذي تم تقليد بطاقة صاحبه، وإذا أردنا الإجابة على السؤال المشار إليه فيتعين التفرقة بين ثلاثة فروض:

الفرض الأول: أن يقوم حامل البطاقة المزورة بتقديمها إلى التاجر

ويفصح له عن طبيعتها، ويقوم هذا الأخير بعد الاتفاق مع حامل البطاقة بقبولها ويتم الوفاء بواسطتها، في هذا الفرض فإن حامل البطاقة لا يسأل عن جريمة استعمال؛ لأنه لم يحتج بالبطاقة على أنها صحيحة، وإنما يسأل كشريك للتاجر الذي يحتج بها على البنك بأنها بطاقة صحيحة، ولا يغير من ذلك التكييف أن التاجر سوف يحتج على البنك بصورة من البطاقة المزورة.

الفرض الثاني: أن يقوم حامل البطاقة المزورة بتقديمها للتاجر على أنها صحيحة، ويعلم هذا الأخير أنها مزورة ولا يفصح لحاملها عن ذلك، ويقبل الوفاء بواسطتها، في هذا الفرض يعد حامل البطاقة مرتكبًا لجريمة الاستعمال، ويعد التاجر كذلك مرتكبًا للجريمة ذاتها؛ إذ إنه سوف يحتج بصورة هذه البطاقة لدى البنك لاستيفاء حقه وهو يعلم أن البطاقة مزورة[1].

الفرض الثالث: أن يكون حامل البطاقة وهو فرض نادر الوقوع غير عالم بأن البطاقة مزورة ويقدمها للتاجر، ويعلم هذا الأخير بتزويرها، وعلى الرغم من ذلك يقوم بقبولها، في هذا الفرض لا يسأل حامل البطاقة عن جريمة الاستعمال لانتفاء القصد الجنائي، ولكن يسأل التاجر عن جريمة الاستعمال إذا استخدمها واحتج بها في مواجهة البنك.

ولا يضيف تجريم هذا النشاط جديدًا إلى حماية بطاقة الوفاء، إلا إذا نفينا صفة التجريم عن مطالبة التاجر للبنك بقيمة المشتريات استنادًا لصورة

(1) نقض 26 يونيو 1956، مجموعة أحكام محكمة النقض، س7 ، رقم 25، ص 91، حيث جاء في حكم محكمة النقض: " فالتاجر سوف يستخدم صورة البطاقة ويحتج بها على البنك، وهذه الصورة تكفي لقيام جريمة الاستعمال إن توافرت بقية أركانها".

بطاقة الوفاء المزورة.

وفي كل الأحوال فهي جريمة خاصة نص عليها المشرع في هذا القانون، وجعل لمرتكبها ذات عقوبة المزور والمستعمل لبطاقة الوفاء المزورة، ويجب تطبيق أحكامها في حالة ثبوت ارتكابها بعناصرها السابقة دون تطبيق القواعد العامة في جريمة استعمال المحررات المزورة.

ثالثًا: الركن المعنوي للجريمة:

يتخذ الركن المعنوي لهذه الجريمة صورة القصد الجنائي العام بشقيه العلم والإرادة، ويتمثل وفقا للقواعد العامة في علم المتهم بعناصر الجريمة واتجاه إرادته إلى ارتكابها، وبتطبيق ذلك على بطاقة الوفاء، فإن القصد الجنائي يتوافر بعلم المتهم بأن البطاقة مزورة أو مقلدة، واتجاه إرادته إلى قبولها كوسيلة وفاء.

الفرع الرابع

العقوبات المقررة لهذه الجرائم

حدد المشرع الفرنسي عقوبتين أصليتين، وعقوبة تكميلية وجوبية، لهذه الجرائم، وسوف نتناول ذلك فيما يلي:

1- العقوبات الأصلية لهذه الجرائم:

جعلها المشرع الحبس مدة لا تقل عن سنة ولا تزيد على سبع سنوات، والغرامة التي لا تقل عن 3600 فرنك ولا تزيد على 500000 فرنك، أو إحدى هاتين العقوبتين[1]، ومن الواضح أن المشرع ترك للقاضي سلطة

(1) جعل المشرع الفرنسي عقوبة التزوير أو استعمال المحرر المزور أو الشروع فيهما الحبس لمدة ثلاث سنوات والغرامة التي مقدارها 300.000 (المادتان 1/44 , 9/44 من قانون العقوبات الفرنسي الجديد).

تقديرية واسعة في تقرير العقاب، وتبدو أهمية ذلك في جريمتي الاستعمال والقبول، ففرق بين من يستعمل البطاقة أو يقبلها للوفاء بمبلغ بسيط، وبين من يستعملها أو يقبلها للوفاء بمبالغ كبيرة.

2- العقوبة التكميلية لهذه الجرائم:

أضاف المشرع إلى العقوبة السابقة عقوبة تكميلية وجوبية هي المصادرة، ويتمثل موضوعها في البطاقات المزورة أو المقلدة، وكذلك المواد والماكينات والمعدات والأدوات التي استخدمت في التزوير أو التقليد أو التي كان مقررًا استخدامها في هذا الغرض إلا إذا كان ذلك بدون علم المالك.

3- حماية حقوق المالك حسن النية:

تفترض هذه الحماية أن الأشياء المستخدمة في التزوير أو التقليد لم تكن مملوكة للمتهم، وإنما قام باستعارتها أو أودعت لديه، ولكنه قام باستخدامها في ارتكاب جريمة التزوير أو التقليد دون علم المالك، في هذه الحالة لا يجوز الحكم بالمصادرة حماية لحقوق المالك الذي لم يعلم بالغرض غير المشروع الذي يبتغي المتهم تحقيقه.

وغني عن البيان أن هذه الحماية تقتصر على الأدوات أو الأشياء المستخدمة في ارتكاب الجريمة، أما نتيجة هذه الجريمة أي البطاقات المزورة أو المقلدة فإنه يتم مصادرتها في كل الأحوال، فهي تأخذ صورة التدبير الاحترازي الذي ينصب على أشياء تخرج بطبيعتها عن دائرة التعامل[1].

(1) ففي في هذه الحالة - وكما قالت محكمة النقض المصرية - فإننا نكون بصدد إجراء بوليس يتعين اتخاذه في مواجهة الكافة. نقض 16 مايو 1966, مجموعة=
= أحكام محكمة النقض, س 17, رقم 112, ص 628.

وأخيرًا فإننا نرى أن الحماية الجنائية في القانون الفرنسي المقررة لتقليد وتزوير بطاقة الوفاء قد اقتصرت على تجريم تزوير البطاقة واستعمالها، أو قبولها مع العلم بتزويرها، ولكنها لم تمتد إلى حالة قيام حامل البطاقة باستخدامها على الرغم من انتهاء صلاحيتها أو إلغائها من جانب الجهة التي أصدرتها، ولا تمتد كذلك إلى حالة الاستخدام التعسفي لبطاقة الوفاء على الرغم من عدم وجود رصيد دائن لحاملها لدى البنك، ولا تمتد هذه الحماية أيضًا للغش الذي يصدر من حامل البطاقة عن طريق الادعاء بفقدها أو سرقتها، ويقوم بإبلاغ الجهة التي أصدرتها بذلك، ثم يستمر هو في استخدامها في السحب أو كوسيلة وفاء.

وهذا المنهج يمكن تبريره بأن أغلب الحالات الأخرى التي يتم فيها استخدام بطاقة الوفاء بطريقة غير مشروعة تخضع للقواعد العامة في قانون العقوبات، سواء تم تكييف نشاط المتهم على أنه سرقة أو نصب أو خيانة أمانة[1]، ومن ناحية ثانية فإنه في الحالات التي لا يخضع فيها نشاط المتهم لتكييف جنائي، وأهمها استعمال بطاقة الوفاء بواسطة حاملها على الرغم من عدم وجود رصيد، فإن هذا النشاط يجب عدم خضوعه لتكييف جنائي وذلك تمشيًا مع سياسة المشرع الفرنسي في جريمة إصدار شيك بدون رصيد التي قام بإلغائها إلا في حالات بسيطة[2].

(1) ETIENNE MADRANGES, La loi du 30 decembre 1991, relative a la securite des cheques et des cartes de paiement, vers un denengorgement des tribunaux, la novelle penalite Liberatoire, G. P. 1992, Doc. P. 3.

(2) وأهمها حالة سحب الرصيد بعد سبق إصدار الشيك ومنع المسحوب عليه من الدفع بعد إصدار الشيك.

فالشيك وبطاقة الوفاء قد أصبحا وسيلتين للوفاء متشابهتين إلى حد كبير، لذا فمن المنطقي إخضاعهما في مجال القانون الجنائي لنظام قانوني واحد[1].

وقد نص قانون مكافحة جرائم تقنية المعلومات الإماراتي على حماية البطاقات الإلكترونية جنائيًا على اعتبار أن البطاقات الإلكترونية - والتي منها بطاقات الائتمان كما رأينا - تعتبر من الوسائل المهمة في الدفع عبر شبكة الإنترنت من خلال التسوق أو التمتع بخدماتها، الأمر الذي يجعلها أكثر خطورة وتعرضًا للاستيلاء عليها من قبل الغير، أو من قبل حاملها، واستخدامها بصورة غير مشروعة.

وجرم القانون في المادة (11) منه استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات بطاقات ائتمانية، أو غيرها من البطاقات الإلكترونية، وعاقب فيها بالحبس وبالغرامة، وإن قصد من ذلك استخدامها في الحصول على أموال الغير أو ما تتيحه من خدمات يعاقب بالحبس مدة لا تقل عن ستة أشهر وبالغرامة أو بإحداهما، وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التي لا تقل عن ثلاثين ألف درهم، أو إحدى هاتين العقوبتين إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على مال الغير.

والمشرع هنا لم يكتف بحماية البطاقات الائتمانية فقط، وإنما شمل جميع البطاقات الإلكترونية، وتشمل هنا البطاقات الخاصة ببعض المواقع والتي تطرح للبيع مقابل التمتع بخدمات هذا الموقع، وكذا البطاقات الخاصة بالاتصال، وغيرها من البطاقات.

---

(1) ومن الجدير بالذكر أن المشرع في القانون رقم 91،1382 قد جرم تزوير الشيك واستعماله أو قبوله مع العلم بتزويره.

والحماية هنا تنصب على أرقام أو بيانات هذه البطاقات إذا ما تم التوصل إليها بدون وجه حق وإن لم تستخدم هذه البيانات، وشدد المشرع في العقوبة في حالة قصد الجاني استخدام هذه البيانات والأرقام في الحصول على أموال الغير أو التمتع بالخدمات، وهنا عاقب على مجرد القصد، فإن استولى الجاني عن طريق ذلك على أموال الغير لنفسه أو لغيره كان التشديد الوارد في الفقرة الأخيرة من المادة، والتي نرى أنها شددت على الحصول على أموال الغير دون التمتع بالخدمات، وهنا نعتقد أن التمتع بهذه الخدمات من شأنه الحصول على أموال الغير بطريقة غير مباشرة.

كما أنه من المتصور قيام القراصنة بإنشاء بطاقات جديدة بواسطة البرامج المخصصة لذلك، والتي تتيح لهم تخليق أرقام بطاقات خاصة بالبنوك أو المواقع، ومن ثم استخدام هذه البطاقات بطريقة غير مشروعة.

وبطاقات الائتمان بصورتها العادية تكاد تثير خلافًا في الفقه حول مدى انطباق النصوص التقليدية عليها، فكيف إذا ما كان هذا الاعتداء قد تم باستخدام الوسائل التكنولوجية الحديثة، وكان الأجدر بالمشرع تناول بطاقات الائتمان بمزيد من الحماية، خاصة وأن قانون العقوبات أو أية قوانين عقابية أخرى لم تبسط الحماية الجنائية عليها، فمتصور أن تكون بطاقة الائتمان عرضة للاعتداء عليها من قبل حاملها الشرعي، وذلك بإساءة استخدامها أثناء مدة صلاحيتها أو بعد انتهاء مدة الصلاحية أو إلغائها، أو تكون عرضة للاعتداء عليها من قبل الغير، وذلك بإساءة استخدامها من قبل الغير في حالة سرقة البطاقة أو تزويرها أو العثور عليها، كما سبق وأن رأينا.

وختامًا نرى ضرورة التدخل التشريعي وإيجاد نصوص خاصة تضفي الحماية الجنائية لبطاقات الائتمان من أي اعتداء يقع عليها سواء من حاملها أو من الغير، أخذًا بالتشريعات التي قامت بذلك، خاصة وأن بطاقات

الائتمان تلعب دورًا كبيرًا في التجارة الإلكترونية، وحمايتها جنائيًا يضفي مزيدًا من الاستقرار على هذه التجارة، ولنا مثال جيد في الجرائم المنصوص عليها في القانون الفرنسي، وإن شابها القصور في بعض الحالات التي تركت للقواعد العامة في قانون العقوبات، حيث اقتصر مجال التجريم على جريمة التقليد أو تزوير بطاقة الوفاء، وجريمة استعمال أو محاولة استعمال بطاقة مقلدة أو مزورة، وجريمة قبول الوفاء بواسطة بطاقة مقلدة أو مزورة.

ومن القوانين العربية التي تصدت لجرائم بطاقات الائتمان القانون العماني، حيث نص في مدونته العقابية بالمادة (276) مكررًا (3) على أن: (يعاقب بالسجن مدة لا تزيد على خمس سنوات وبغرامة لا تجاوز ألف ريال كل من:

1) قام بتقليد أو تزوير بطاقة من بطاقات الوفاء أو السحب.

2) استعمل أو حاول استعمال البطاقة المقلدة أو المزورة مع العلم بذلك.

3) قبل الدفع ببطاقة الوفاء المقلدة أو المزورة مع العلم بذلك.

كما تنص المادة (276) مكررًا (4) على أنه: "يعاقب بالسجن مدة لا تزيد على 3 سنوات وبغرامة لا تجاوز خمسمائة ريال كل من:

1) استخدم البطاقة كوسيلة للوفاء مع علمه بعدم وجود رصيد لها.

2) استعمل البطاقة بعد انتهاء صلاحيتها أو إلغائها وهو عالم بذلك.

3) استعمل بطاقة الغير بدون علمه.

وفي كندا اعتبر قانون العقوبات في المادة (321) الاستعمال غير المشروع متحققًا سواء تم استخدامها على نحو غير مشروع كبطاقة وفاء للحصول على خدمات أو بضائع أو أي شيء آخر له قيمة، أو كبطاقة سحب تسمح بالدخول إلى الخدمات المختلفة التي تقدمها أجهزة الصرف الآلي.

وفي سويسرا ترك قانون العقوبات تجريم إساءة استعمال البطاقة من قبل الغير للمادة (147) والخاصة بالاحتيال المعلوماتي، ونص صراحة على الاستعمال غير المشروع للبطاقة من قبل حاملها في المادة (148).

وفي الولايات المتحدة الأمريكية يوجد منذ 1984 نص يتناول الاستعمال غير المشروع لبطاقات الائتمان في المادة (1029) من القانون الفيدرالي والمعدل عام 1994، ويجرم هذا النص الاستعمال التعسفي للأدوات التي تسمح بالدخول إلى حساب بنكي ويمكن من خلالها الحصول على أموال أو أشياء أو خدمات أو أي شيء آخر له قيمة، كما يشمل النص الاستعمال غير المصرح به لمثل هذه الأدوات كالبطاقات المسروقة أو المفقودة أو منتهية الصلاحية أو الملغاة، وكذا تزوير وتقليد البطاقات، أو حيازة الأجهزة التي تساعد على تقليد أو تزوير البطاقات[1].



(1) د. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، مرجع سابق، ص 605.

المبحث الثالث

الجرائم المتعلقة بمزود خدمة المصادقة الإلكترونية

تعد مرحلة التصديق على التوقيع الإلكتروني من أهم مراحل إبرام عقود التجارة الإلكترونية، نظرًا لما لهذه المرحلة من أهمية بارزة في إثبات العقد والتأكد من مضمونه وصحة ما ورد به من بيانات، بالإضافة إلى التأكد من صحة التوقيع الوارد عليه ونسبته لصاحبه، ويتولى عملية التوثيق الإلكتروني أو المصادقة الإلكترونية وسيط مستقل ومحايد تحدده الدولة وتعترف به.

وتأتي أهمية القائمين على منح شهادات تصديق البيانات الإلكترونية من أن المعاملات الإلكترونية حتى يتم التعامل فيها والتوقيع بما يمكن من نسبتها لمن قام بها من قبل أي شخص يريد الدخول في هذه المعاملات، تحتاج إلى شخص آخر للتأكد من صحة ومصداقية هذه المعلومات.

وبالاستناد إلى الشهادات الصادرة عن هذا الشخص والذي يسمى مزود خدمة التصديق تدخل مختلف الأطراف في معاملات مالية وتجارية بطرق إلكترونية، وعليه فإن مصداقية هؤلاء الأشخاص هي أساس المصداقية في التجارة الإلكترونية ذاتها.

ولقد اهتمت التشريعات الوطنية ببحث الوضع القانوني لهؤلاء الأشخاص، ودورهم في إتمام المعاملات الإلكترونية، وكذلك الحجية المترتبة على شهادات التصديق الأجنبية لدى السلطة الوطنية، وسوف نتناول موضوع المصادقة الإلكترونية في مطلبين، نخصص الأول للحديث عن مزودي خدمة المصادقة، وخضوعهم للقانون بشأن توثيق التوقيع الإلكتروني، والثاني في المسئولية الجنائية لمزودي خدمة المصادقة الإلكترونية.

المطلب الأول: مزودو خدمة المصادقة الإلكترونية ومدى التزامهم بالقانون

المطلب الثاني: المسئولية الجنائية لمزود الخدمة أو مقدمها

المطلب الأول

مزودو خدمة المصادقة الإلكترونية ومدى التزامهم بالقانون

يعرف مقدم خدمة المصادقة الإلكترونية بأنه جهة أو منظمة عامة أو خاصة مستقلة محايدة، تقوم بدور الوسيط بين المتعاملين لتوثيق تعاملاتهم الإلكترونية بإصدار شهادات المصادقة الإلكترونية، ويتم تدخل الموثق الإلكتروني بناءً على طلب الأطراف بهدف إنشاء وحفظ وإثبات الرسائل الإلكترونية[1].

وقد عرف التوجيه الأوروبي رقم 99/6229 في المادة 2/ 6 هذه الجهات بأنها: "كل شخص قانوني طبيعي أو معنوي يصدر شهادات توثيق التوقيع الإلكتروني أو يتولى تقديم خدمات أخرى مرتبطة بالتوقيع الإلكتروني "[2]، وهو التعريف ذاته الذي أورده قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية.

وقد عرفت المادة (1) من قانون المعاملات والتجارة الإلكترونية الإماراتي مزود خدمة المصادقة الإلكترونية بأنه: "أي شخص أو جهة معتمدة أو معترف بها، تقوم بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمات متعلقة بها وبالتوقيعات الإلكترونية والمنظمة بموجب أحكام هذا القانون".

(1) د. سعيد السيد قنديل، التوقيع الإلكتروني، مرجع سابق، ص 75.

(2) http://jya.com/eu.difsig3.htm

يذكر أن هذا التعريف يتطابق مع التعريف الوارد في القانون رقم (2) لسنة 2002م بشأن المعاملات والتجارة الإلكترونية المعمول به في إمارة دبي، حيث عرفت المادة (2) من القانون مزود خدمات التصديق بأنه: "أي شخص أو جهة معتمدة أو معترف بها، تقوم بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمات متعلقة بها وبالتوقيع الإلكتروني".

ونظرًا لدور مزودي الخدمة الوسيطة في شبكة الإنترنت وتأثيرها البالغ في التجارة الإلكترونية، فقد صدر عن الاتحاد الأوروبي التوجيه رقم 31/2000 بتاريخ الثامن من يونيو عام 2000م، وعالج بعض الجوانب القانونية للتجارة الإلكترونية، وقد نصت المادة (40) من هذا التوجيه على ضرورة توحيد المعاملة القانونية بالنسبة لمسئولية الوسطاء الذين يقدمون خدمة شبكة الإنترنت ومزودي خدمات المصادقة الإلكترونية، وذلك لأن الاختلاف التشريعي في معالجة هذه المسألة يعيق التجارة الداخلية أو الخارجية، وأنه يجب على الوسطاء في خدمة شبكة الإنترنت، الكف عن أية أعمال غير مشروعة ووقفها، وعلى الدول الأعضاء الالتزام بمجموعة من الوسائل السريعة والفعالة.

فالمعاملات الإلكترونية من أجل التعامل بها والتوقيع بما يفيد صحة صدورها عمن قام بها يوقع عليها إلكترونيًا، كما أن أي شخص يريد الدخول في هذه المعاملات لابد له من التأكد من صحة هذه المعلومات ومصداقيتها، ومن هنا تأتي أهمية الأشخاص القائمين على منح شهادات تصديق البيانات الإلكترونية، الذين يطلق عليهم اسم مزودي خدمة التصديق، وقد عرف مزود خدمات المصادقة الإلكترونية بأنه "كل شخص طبيعي أو اعتباري ينشئ ويسلم ويتصرف في شهادات المصادقة

الإلكترونية، ويقدم خدمات أخرى ذات علاقة بالتوقيع الإلكتروني[1]".

كما عرفت شهادة المصادقة الإلكترونية بأنها: "رسالة بيانات أو أية وثيقة أخرى تؤكد الارتباط بين الموقع وبيانات إنشاء التوقيع".

وحتى يقوم مزود خدمات المصادقة الإلكترونية بعمله في إصدار شهادات المصادقة الإلكترونية في شأن البيانات والمعاملات المتداولة في المعاملات والعقود الإلكترونية عن طريق إصدار شهادات رقمية، فهو ملزم باتباع خطوات فنية وإدارية معينة إلى أن تصدر هذه الشهادة، فضلا عن قيام المزودين بتوفير كوادر بشرية فنية ومحاسبية وإدارية لديهم قدرة على إنجاز منظومة العمل، ولذلك يعهد إلى جهات محلية حكومية بإصدار اللوائح والشروط التي تنظم عمل مزودي الخدمة.

ففي قانون المعاملات والتجارة الإلكترونية الإماراتي نصت المادة 20 على أنه: "لأغراض هذا القانون يعين بقرار من مجلس الوزراء جهة لمراقبة خدمات التصديق، وعلى وجه الخصوص لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي خدمات التصديق والإشراف عليها". وأورد قانون المعاملات والتجارة الإلكترونية عددًا من الواجبات في شأن مزود خدمات التصديق الذي يمنح شهادات المصادقة الإلكترونية التي يعتمد عليها ذوو الشأن في إتمام معاملاتهم الإلكترونية.

وتقسم هذه الواجبات القانونية إلى واجبات عامة محددة تتعلق بالثقة في النظم والإجراءات والموارد البشرية، وتلك التي تتعلق بمضمون الشهادة، وإلى مجموعة من الأحكام التي تلزم مزود خدمات المصادقة الإلكترونية باتباع خطوات فنية وإدارية معينة لإصدار شهادة المصادقة، فضلا عن

(1) قانون المعاملات والتجارة الإلكترونية الإماراتي رقم 2006/1 الفصل الأول، المادة (1) تعاريف.

ضرورة توافر كوادر بشرية وفنية ومحاسبية وإدارية لديها القدرة على إنجاز منظومة العمل، ولذلك يعهد إلى جهات حكومية وطنية بإصدار اللوائح والشروط التي تنظم عمل مزودي خدمات المصادقة.

ففي قانون المعاملات والتجارة الإلكترونية، تختص الجهة المعينة بقرار من مجلس الوزراء بمراقبة خدمات التصديق الإلكترونية لأغراض ترخيص وتصديق ومراقبة أنشطة مزودي الخدمة والتصديق والإشراف عليها[1].

المطلب الثاني

المسئولية الجنائية لمزود الخدمة أو مقدمها

يتطلب موضوع الحماية الجنائية للتجارة الإلكترونية البحث في موضوع مسئولية من يقومون بخدمات وسيطة تتعلق بتوصيل خدمة شبكة الإنترنت، أو إيواء المعطيات أو البيانات الخاصة بشبكة الإنترنت عند التعامل، ومدى مساءلتهم عما يقع من الغير من جرائم[2]، ويمكن حصر مقدمي الخدمات الوسيطة الخاصة بشبكة الإنترنت في ناقل ومورد المعلومات، ومتعهد الوصول، ومتعهد الخدمات، فناقل المعلومة يتولى مهمة النقل المادي لها بوسائله الفنية، بحيث يقوم بالربط بين الشبكات، تنفيذًا لعقد نقل المعلومات بين الحاسبات المرتبطة بمواقع شبكة الإنترنت أو بمستخدمي الشبكة، وتتولى تلك المهمة عادة الهيئة المسئولة عن الاتصالات، بحيث تتعاقد عادة

(1) أصدر مجلس الوزراء القرار الوزاري رقم 291/8 لعام 2006 بتاريخ 2006/10/15 بشأن تعيين الهيئة العامة لتنظيم قطاع الاتصالات كمراقب لخدمات التصديق الإلكتروني، كما أصدر وزير الاقتصاد القرار الوزاري رقم (1) لسنة 2008 بشأن إصدار لائحة مزودي خدمات التصديق الإلكتروني.

(2) 16 eem hournèes huridiques fanco، italienne، cormayeur, 10، 13 juin 1999, revue international du driot coparè. N 4 , 1999 , P. 127.

مع مورد خدمات شبكة الإنترنت والمشروعات والمنظمات صاحبة الاشتراكات على الشبكة العامة أو تستأجر خطوطًا متخصصة عليها[1]، ويجب الالتزام بسرية المراسلات عبر شبكة الاتصالات، والحياد تجاه مضمون الرسائل المنقولة[2].

وينبغي التمييز بين مزود الخدمة وغيره من المزودين والموردين في المجال المعلوماتي، فمزود الخدمة هو من يقوم الأفراد عن طريقه بالاتصال بشبكة الإنترنت، إذ يعد وسيطًا بين مستخدم شبكة الإنترنت ومورد الخدمات التي يتعهد بها عبر عقود الاشتراك التي يبرمها، وعن طريقه يتم اتصال مستخدمي شبكة الإنترنت بالمواقع التي يرغبون في الدخول عليها[3].

ومورد المعلومة هو شخص طبيعي أو معنوي يتوسط بين مؤلف مضمون الموقع ومستخدم شبكة الإنترنت الذي يرغب في الاطلاع على ذلك الموقع، فهو يقوم بتحميل النظام بالمعلومات التي قام بتأليفها أو جمعها حول موضوع معين، أي أنه يتولى الاختيار والتجميع والتوريد للمادة المعلوماتية حتى تصل إلى الجمهور عبر الشبكة[4].

أما متعهد الإيواء فهو شخص طبيعي أو معنوي يتولى تخزين التطبيقات والسجلات المعلوماتية لعملائه، ويمدهم بالوسائل التقنية والمعلوماتية التي تمكنهم من الوصول إلى ذلك المخزون عبر شبكة الإنترنت على مدار اليوم، وعرفت مسئولية متعهد الإيواء جدلا كبيرًا خلال

(1) د. محمد حسين منصور، المسئولية الإلكترونية، مرجع سابق، ص 197.
(2) Art L. 34 du code FRANCIAS des postes et des communications électroniques.
(3) د. محمد عبد الظاهر حسين، المسئولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، 2002، ص37.
(4) د. محمد حسين منصور، المسئولية الإلكترونية، مرجع سابق، ص 199.

الكتابات الفقهية وأحكام القضاء، التي تغلب إعفاء متعهد الإيواء من المسئولية عن فعل الغير، ويتحمل فقط خطأه الثابت.

أما متعهد الوصول فهو كل شخص طبيعي أو معنوي يقدم للعملاء الراغبين من الجمهور خدمة الوصول إلى شبكة الإنترنت.

ومتعهد الخدمات هو مصدر التدفق المعلوماتي، فهو بمثابة ناشر الموقع، وتثور المسئولية الجنائية لمتعهد الخدمات عن المعلومات المزيفة والناقصة والفاضحة التي يعدها وينشرها على موقعه لأنه قادر عمليًا على السيطرة على المعلومات والتحكم في نشرها[1].

وقد أثارت المسئولية الجنائية لمزود الخدمة وغيره من مقدمي الخدمات الوسيطة، الكثير من الجدل في الفقه، والذي انقسم إزاءها إلى عدة آراء، حيث يرى البعض عدم قيام المسئولية الجنائية في أي حال من الأحوال، بينما ذهب آخرون إلى قيام المسئولية الجنائية ضد مزود الخدمة[2].

وبالنظر للقانون المقارن نجد أن الولايات المتحدة الأمريكية واجهت مثل هذه المشكلة وذلك حين أصدر المشرع الأمريكي في 8 فبراير 1996 قانون آداب الاتصالات، بقصد مواجهة تفشي الإباحية في وسائل الاتصال العامة ومن بينها شبكة الإنترنت، وقد تضمن هذا القانون أحكامًا مختلفة تعاقب على بث المشاهد الفاحشة أو الإباحية؛ إذ حظر عرض المشاهد أو الصور الفاحشة أو الفاضحة حسب قواعد المجتمع المعاصر.

لكن ورود هذه العبارات في القانون أثار حالة من الارتياب ونقاشًا عارمًا في أوساط عدد من المحاكم الأمريكية التي اعتبرت إحداها بأن عبارتي فاحشة (Indecent) وفاضحة Monifestement)

(1) المرجع السابق، ص 218.
(2) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 121.

choquants) غير دستورية، وذلك بعد أن استفاضت في إجراء تحليل مسهب لخصوصيات الاتصال بواسطة شبكة الإنترنت[1].

وسوف نتناول المسئولية الجنائية لمقدمي الخدمات وفقًا لما وردت في التوجيه الأوروبي، والتشريعات الوطنية سواء أكانت أجنبية أو عربية، وذلك على النحو التالي:

أولا: المسئولية الجنائية في ظل التوجيه الأوروبي رقم 31/2000

أكد التوجيه الأوروبي في المادة (40) بشأن بعض الجوانب القانونية للتجارة الإلكترونية[2] أن الاختلاف بين قوانين الدول الأعضاء بشأن مسئولية مقدمي الخدمات باعتبارهم من الوسطاء يعوق التجارة الداخلية والخارجية؛ لأنه يخلق اختلالا في سوق المنافسة، وأنه يتعين على مقدمي هذه الخدمات واجب العمل على وقف الأنشطة غير المشروعة أو وضع حد لها، ولذلك كان من المتعين أن يكون هذا التوجيه أساسًا ملائمًا لإعمال وسائل سريعة وفعالة لمنع الأنشطة غير المشروعة ووقفها، وكان من مصلحة الجميع اعتماد هذه الوسائل والأساليب[3].

كما أنه لا يسأل قانونًا إذا كان عمله يقتصر على النقل أو التخزين، أي عندما لا يساهم بأية صورة كانت في البيانات المنقولة، وبما يفترض عدم تدخله في تعديلها، أما التدخل الفني الخاص بعملية النقل فلا يثير المسئولية.

---

(1) د. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، مرجع سابق، ص 170.

(2) Directive 2000/31 du parlement européen et du conseil, du 8 juin 2000 relative a certains aspects juridique des services de la société de information et notamment du commerce électronique dans le merchè intèrieur (directive sur le commerce électronique) voir le site: www.europa.eu.int.

(3) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، دار النهضة العربية، 2001، ص 122.

حيث إنه لا يمثل تدخلا في المعلومات والبيانات ذاتها. (المادة (43) من التوجيه).

وفيما يتعلق بمن يقوم بخدمة تخزين البيانات فإنه ملزم بمجرد علمه بعدم مشروعية البيانات المخزنة بالقيام بحبسها أو منع الوصول إليها. (المادة (46) من التوجيه)، وعلى مقدم الخدمة أن يضع حدًّا لمخالفة قانونية أو أن يخطر بأي مخالفة وقعت (مادة 12 فقرة 3).

وقد قررت المادة (14) عدم مسئولية متعهد الإيواء عن البيانات التي يقوم بإيوائها بناءً على طلب العملاء بشرط ألا يكون عالمًا بعدم مشروعية البيانات، أما إذا علم بذلك فيجب اتخاذ اللازم لمنع الاطلاع عليها أو سحبها، وذلك مع عدم الإخلال بحق الجهات الإدارية أو القضائية في الدول الأعضاء في توجيه مقدم الخدمة لمنع نقل أي بيانات غير مشروعة أو الإخطار بوجود مثل هذه البيانات[1].

ثانيا: المسئولية الجنائية في التشريعات الوطنية.

1- القانون الفرنسي:

تمت الاستعانة بتجربة (التيليماتيك) أو شبكة المينيتيل (Minitel) التي سبقت استخدام شبكة الإنترنت في فرنسا بسنوات عدة، واعتبرت أن شبكة الإنترنت من بين هذه الخدمات، وأنها تخضع لقانون الاتصال عن بعد الصادر في 30 سبتمبر 1986 على اعتبار أنها تؤلف خدمات سمعية وبصرية وفق المعنى المبين في هذا القانون[2].

وقد نص هذا القانون على أنه يقع على عاتق متعهد الخدمة الالتزام

(1) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 123.
(2) د. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، مرجع سابق، ص 172.

بحسن تنفيذ الخدمة المعلوماتية، بحيث يتم تنفيذها بما يتفق مع أعراف المهنة، ويلتزم أيضًا بالإعلام عن وسائل الدخول إلى الخدمة مثل شفرة تحقيق الهوية، ويقوم بمراقبة محتوى الرسائل التي تصل إليه، ويقرر عدم نشر تلك التي يقدر أنها غير مشروعة[1].

وقانون الاتصال تم تعديله في عام 1996 بتعديل سمي تعديل (Fillon) على اسم وزير البريد والاتصالات في ذلك الحين، وهذا التعديل يتعلق بتكليف المجلس الأعلى للتيليماتيك بإصدار توصيات تهدف إلى ضمان احترام مجموعة من قواعد الآداب المهنية المتناسبة مع طبيعة الخدمات المقدمة من قبل موردي خدمات الاتصالات السمعية والبصرية الداخلة ضمن نظام التصريح المسبق، ومن بينهم موردو خدمات الاتصال بشبكة الإنترنت.

كما نصت مواد التعديل إنشاء هيئة خاصة تابعة للمجلس الأعلى للتيليماتيك مهمتها إصدار آراء حول مطابقة خدمات الاتصالات السمعية والبصرية لمضمون التوصيات الصادرة.

ولكن المجلس الدستوري أبطل هذه الأحكام المتعلقة بوضع التوصيات والآراء، استنادًا إلى عدم دستوريتها ومخالفتها لنص المادة (34) من الدستور الفرنسي المتعلق بالحقوق المدنية والضمانات الأساسية الممنوحة للمواطنين في ممارسة الحريات العامة ولاسيما حرية التعبير، والمؤكدة أيضًا في المادة (11) من الإعلان العالمي لحقوق الإنسان.

والمجلس الدستوري في قراره السابق أخذ على المشرع الفرنسي عدم تعريفه للمبادئ الواجب احترامها من أجل وضع هذه التوصيات والآراء، لكنه أبقى على الفقرة في القانون التي تلزم موردي خدمات الاتصال تجاه

(1) د. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، مرجع سابق، ص 162.

زبائنهم باقتراح وسائل تقنية معروفة باسم برامج فلترة المواقع Filtragedes sites تسمح لهم بإجراء اختيار أو انتقاء للخدمات التي يرغبون بالوصول إليها، واقتراح وسائل مماثلة على المشتركين تمنع الاتصال أو الوصول إلى عدد من الخدمات أو المواقع[1].

هذا وقد أصدر قسم التقارير والدراسات بمجلس الدولة الفرنسي- تقريرًا في شأن شبكة الإنترنت والخطوط الرقمية والذي وافقت عليه الجمعية العمومية للمجلس في الثاني من يوليو 1998[2]، ويعد هذا التقرير من أبرز الأعمال التي صدرت في فرنسا، والتي تعرضت للمشكلات القانونية الخاصة بشبكة الإنترنت والتجارة الإلكترونية، ومن بين الموضوعات التي تناولها التقرير بشكل مفصل موضوع المسئولية القانونية لمقدمي الخدمات الوسيطة بشبكة الإنترنت.

وقد أوضح التقرير المذكور أن تحديد مسئولية العاملين في مجال شبكة الإنترنت من المسائل المهمة لوضع تنظيم يتعلق بشبكة الإنترنت، وأن المسئولية الجنائية المفترضة والمطبقة في مجال الاتصالات السمعية والبصرية لا تصلح لإقامة مسئوليتهم.

واعتمد التقرير إعفاء مقدمي الخدمات الوسيطة من المسئولية إلا إذا ثبت توافر علمهم بالمحتوى أو ساهموا في ارتكاب الجريمة، وقد يؤدي ذلك إلى تزايد الظاهرة الإجرامية.

ويؤكد التقرير كذلك على ضرورة تعميم الأحكام العامة للقانون الجنائي، بحيث يمكن مساءلة القائم بالأعمال المتعلقة بشبكة الإنترنت، سواء باعتباره

---

(1) د. طوني ميشال عيسى، التنظيم القانون لشبكة الإنترنت، مرجع سابق، ص 174.

(2) Conseil d état: Internet et les résaux numériques, étude adoptée par l assemblée génale de conseil d état le 2 juillet 1998, section de rapport t des études. Voir le site: www.internet.gov.fr.

فاعلا أصليًا أو فاعلا مع غيره أو مساهمًا تبعيًا، طالما قام عمدًا بوضع العمل غير المشروع تحت تصرف الجمهور، وتحديد المسئولية الجنائية يقوم عندئذ على فحص وسائل وإمكانية تدخل الوسيط ومعرفته للجريمة، ومدى قيامه بوضع الوسائل اللازمة لمنع تحققها.

بالإضافة إلى أن المسئولية الجنائية عن الصحافة والنشر ترتبط بتوافر هيئة للتحرير، وهي فكرة بعيدة عن عالم شبكة الإنترنت، ويجب لقيام المسئولية الجنائية للوسطاء أن نأخذ في الاعتبار معرفة المضمون غير المشروع، وتوافر القصد الجنائي، والإجراءات المتخذة لمراقبة هذا النشاط، والقدرة على المراقبة.

ويجب إقامة مسئولية موزع خدمة شبكة الإنترنت في ضوء الأحكام العامة للقانون الجنائي، وليس على أساس المسئولية الجنائية المفترضة وفقًا لقانون الصحافة الفرنسي- أو قانون الإذاعة المرئية أو المسموعة الفرنسي.

وقد تم حسم هذا الموضوع على المستوى القضائي، حيث قضت محكمة استئناف باريس[1] بمسئولية الشخص الذي يقوم بإيواء المواد المتعلقة بشبكة الإنترنت على أساس أن هذه الخدمة من قبيل الخدمات السمعية والبصرية، وأقامت مسئوليته على أساس من المسئولية التلقائية والتي يفترض أنها تتعلق بجرائم الصحافة[2].

وقد أثار هذا الحكم الكثير من الجدل، ولذلك تدخل المشرع الفرنسي لتأكيد الرأي المخالف، وتم تعديل قانون 30 سبتمبر 1986 في شأن حرية

(1) Ca paris, 10 Ferrier 199. D. 1999 , Hurl. 389, Note Nathalie Mallet، polio.

(2) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 130.

الاتصال والذي قرر عدم قيام المسئولية المدنية أو الجزائية للأشخاص الاعتبارية أو الطبيعية، التي تقوم بدون مقابل أو بمقابل بالتخزين المباشر والدائم، لتضع تحت تصرف الجمهور إشارات أو كتابة أو صورًا أو صوتًا أو رسائل أيًا كانت طبيعتها عن محتوى هذه الخدمات، إلا إذا تم إخطارها من قبل سلطة قضائية ولم تقم باتخاذ اللازم لمنع الوصول للمحتوى[1].

2- القانون الألماني:

يحدد التشريع الألماني باعتباره أول تشريع أوروبي مسئولية الوسطاء في شبكة الإنترنت وذلك بمقتضى القانون الصادر في الأول من أغسطس 1997، حيث اهتم بتحديد الأعمال التقنية الوسيطة في مجال شبكة الإنترنت، وقرر عدم مسئولية من يقومون بهذه الأعمال إلا في أحوال محددة على سبيل الحصر والإحالة للقواعد القانونية العامة عند قيام مسئوليته، ولم يلجأ إلى تقرير عدم مسئوليتهم أو إقامة المسئولية على نمط المسئولية عن جرائم الصحافة، ولذلك كان الهدف من التشريع هو إخضاع الأشخاص الذين يعملون كوسطاء في مجال شبكة الإنترنت لقواعد القانون العامة، سواء من الناحية المدنية أو الجنائية أو الإدارية.[2]

3- في دوقية لوكسمبورج:

نظم قانون التجارة الإلكترونية لدوقية لوكسمبورج لسنة 2000 مسئولية مقدمي الخدمات الوسيطة، بحيث قرر عدم مسئولية من يقوم بالنقل بواسطة وسيلة من وسائل الاتصالات، وعدم مسئولية من يقدم خدمة الاتصال بشرط

(1) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 131.

(2) Cyril rojinsky: commerce électronique et responsabilité des acteurs de l'intente en Europe. Voir le site: www.doit.technologiir.org.

ألا يكون هو مصدر المعلومات، وألا يكون هو الذي اختار المصدر، وألا يكون قد قام باختيار أو تعديل المعلومات محل النقل (مادة 60 9).

وقررت المادة (62) من القانون عدم مسئولية من يقدم خدمة الإيواء عن تخزين المعلومات لحساب الغير طالما أنه لا يعلم بعدم مشروعية هذه المعلومات، وإذا علم بمضمونها قام بحبسها أو منع الوصول إليها، وقد قررت المادة نفسها عدم وجود التزام عام على مقدمي الخدمات السابقة بمراقبة المعلومات التي يقومون بنقلها أو تخزينها، وقد وضع المشرع في المادة (63) على عاتق من يقوم بالإيواء التزامًا بمراقبة وقوع بعض الجرائم، مع عدم الإخلال بحق السلطات القضائية في طلب المراقبة لأسباب تتعلق بالأمن أو الدفاع أو الأمن العام أو بمنع الجرائم أو الكشف عنها.

4- القانون التونسي:

يتضمن قانون المعاملات والتجارة الإلكترونية التونسي لسنة 2000 بعض النصوص التي تعنى بمسئولية مقدمي الخدمات الوسيطة الخاصة بشبكة الإنترنت جنائيًا، وأبرز هذه النصوص في رأينا المواد 45، 46، 52، وهذه المواد تعاقب على جريمة عدم مراعاة المواصفات من قبل مزود الخدمة (أ) وجريمة التعامل في بيانات التجارة الإلكترونية بدون ترخيص (ب) ثم جريمة إفشاء الأسرار (ج).

أ - جريمة عدم مراعاة المواصفات من قبل مزود الخدمة:

جاء نص المادة 45 من القانون التونسي بمعاقبة مزود خدمات المصادقة الإلكترونية سواء أكان شخصًا طبيعيًا أم معنويًا بالغرامة التي تتراوح ما بين 1000 و10.000 دينار في حالة عدم مراعاته مقتضيات كراس الشروط المنصوص عليه بالمادة (12) من القانون، ويضاف إلى عقوبة الغرامة عقوبة أخرى منصوص عليها في المادة (44) من هذا

القانون، وهي وقف نشاط مزود الخدمة وسحب الترخيص الخاص به والممنوح له من قبل الوكالة الوطنية للمصادقة الإلكترونية.

ويتمثل الركن المادي - مثلما سبق وأن رأينا - لهذه الجريمة في عدم مراعاة مزود خدمة المصادقة للشروط والمقتضيات المنصوص عليها في كراس الشروط حسب المادة (14) من القانون التونسي.

ويتوافر السلوك الإجرامي لمزود الخدمة بمجرد عدم القيام بعمل من الأعمال المتضمنة في كراس شروط خدمات المصادقة، وهذه الأعمال وفقًا لنص المادة (12) هي كافة دراسات ومتابعات ملفات طلبات الشهادات، وأجل دراسة الملفات، والإمكانيات المادية والمالية والبشرية التي يجب توافرها للقيام بالنشاط، وشروط تأمين التفاعل المتبادل لنظم المصادقة، وربط سجلات شهادات المصادقة، والقواعد المتعلقة بالإعلام والخاصة بخدمات مزود الخدمة والشهادات التي سلمها، والتي يجب على مزود خدمات المصادقة الإلكترونية حفظها[1].

ب - جريمة التعامل في بيانات التجارة الإلكترونية بدون ترخيص:

نصت المادة (46) من القانون التونسي على أنه: "يعاقب كل من يمارس نشاط مزود خدمات المصادقة الإلكترونية بدون الحصول على ترخيص مسبق طبقًا للمادة (11) من هذا القانون بالسجن لمدة تتراوح بين شهرين وثلاث سنوات، وبخطية تتراوح بين 1000 و10000 دينار، أو بإحدى هاتين العقوبتين.

وقد سبق الحديث عن هذه الجريمة، ورأينا أن الركن المادي في الجريمة يتحقق بمجرد التعامل في بيانات التجارة الإلكترونية بدون ترخيص

(1) د. عبد الفتاح بيومي حجازي، مقدمة في التجارة الإلكترونية العربية، مرجع سابق، ص 258.

من الجهة المختصة، ذلك أن معظم الدول تضع في اعتبارها ضرورة وجود جهة تصدر الترخيص أو الإذن بالتعامل في البيانات المعلوماتية لدى هذه النظم[1].

وتشترط المادة (11) من القانون التونسي ضرورة منح الترخيص من الوكالة التونسية للمصادقة، وأوردت المادة (11) شروطًا محددة لمن يُمنح رخصة مزاولة هذا العمل، وعليه إذا قام مزود الخدمة بالتعامل بالمخالفة للمادة (11) قامت الجريمة المذكورة في المادة (46) من هذا القانون.

وبالنسبة للركن المعنوي، رأينا أن هذه الجريمة عمدية، ويجب لقيامها توافر القصد العام بعنصريه العلم والإرادة.

والجاني يعاقب بالسجن لمدة شهرين إلى ثلاث سنوات، وغرامة تتراوح ما بين 1000 و10000 درهم، أو إحدى العقوبتين حسب السلطة التقديرية لمحكمة الموضوع.

ج - جريمة إفشاء الأسرار:

تضمنت المادة (52) من القانون التونسي النص على هذه الجريمة، فنصت على أنه: " يعاقب طبقًا لأحكام الفصل (254) من المجلة الجنائية مزود خدمات المصادقة الإلكترونية وأعوانه الذين يفشون أو يحثون أو يشاركون في إفشاء المعلومات التي عهدت إليهم في إطار تعاطي نشاطاتهم، باستثناء تلك التي رخص صاحب الشهادة كتابيًا أو إلكترونيًا في نشرها أو الإعلام بها، أو في الحالات المنصوص عليها في التشريع الجاري العمل به". ويشترط في البيانات والمعلومات التي يتم إفشاؤها أن تتعلق بالشخص صاحب المعاملة الإلكترونية، ويستوي في ذلك أن تتعلق بحياته العائلية أو

(1) د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص 273 وما بعدها.

سمعته أو باعتباره أو مركزه المالي أو الائتماني، ومن ناحية أخرى يشترط الإدلاء بهذه المعلومات والبيانات إلى شخص لا علاقة لـه بهـذه البيانـات أو المعلومـات والبيانـات، وقـد عاقـب القـانون التونسي على إفشاء المعلومات أو المشاركة في عملية الإفشاء أو التحريض عليها، وهذا يعني رغبة المشرع التونسي في تحقيق حماية جنائية فاعلة لكل بيانات التجارة الإلكترونية.

والركن المادي هنا يتمثل في إفشاء هذه المعلومات أو الأسرار بمعنى إذاعتها أو نقلها وإطلاع الغير عليها، وإعلانها وخروجها من حيز الكتمان أو السرية بعد أن كان العلم بها قاصرًا على أصحابها أو الذين ائتمنوا عليها بحكم وظيفتهم، وهم في هذه الجريمة مزودو خدمة المصادقة الإلكترونية ومعاونوهم، ويستوي في المعلومات التي يتم إفشاؤها أن تكون مكتوبة في أوراق، أو مسجلة على دعامة إلكترونية على شريط مرن أو قرص مدمج، أو أن تكون مخزنة ضمن برنامج معلوماتي في جهاز حاسب آلي، واطلع عليها مزود الخدمة أو معاونوه عند القيام بعملهم.

أما الركن المعنوي، فمن الواضح من صياغة المادة (52) أن جريمة إفشاء المعلومات والأسرار لا تقع إلا بطريق العمد، حيث إن صور الركن المادي في هذه الجريمة هي أفعال الإفشاء أو المشاركة في الإفشاء أو التحريض على الإفشاء والمساعدة فيه.

وبتمام الركن المادي والمعنوي نجد أن المشرع التونسي لم ينص على عقوبة محددة على الجاني في هذه الجريمة، إنما أحال في ذلك إلى القواعد العامة للعقوبة على جريمة إفشاء الأسرار، والمنصوص عليها بالمادة (254) من قانون المجلة الجنائية التونسي[1].

(1) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية العربية، مرجع سابق، ص 280 وما بعدها.

5- التشريع المصري:

يتعين البحث عن مدى توافر هذه المسئولية وفقًا للقواعد العامة في قانون العقوبات بسبب عدم وجود أحكام للقضاء تتعلق بالمسئولية الجنائية للوسطاء في خدمة توزيع شبكة الإنترنت، علمًا بأنه لا يمكن تطبيق القواعد العامة التي تحكم جرائم الصحف أو تلك التي تقع بطريق النشر؛ لأن تعبير الصحيفة حتى الآن في مصر يرتبط بفكرة المطبوع، ولا يشمل المادة المعلوماتية التي تبث بطريق شبكة الإنترنت، وبالتالي يجب هنا تطبيق القواعد العامة في قانون العقوبات، ونلاحظ أن مشروع قانون التجارة الإلكترونية المصري لم يتضمن معالجة مسألة المسئولية الجنائية لموزع شبكة الإنترنت في حالة ارتكاب هذا الأخير لجريمة وفقًا لأحكام هذا القانون.

لكن المشروع تضمن نصًا يمكن أن يطبق على مسئولية موزع شبكة الإنترنت، وهو نص المادة (29) والذي ورد فيه: "مع عدم الإخلال بأي عقوبة أخرى أشد يعاقب بالحبس مع الشغل كل من استخدم نظامًا أو برنامجًا للحيلولة دون إتمام المعاملات التجارية بالوسائل الإلكترونية، وذلك بالتعديل فيها أو محو بياناتها أو إفسادها أو تدميرها أو بتعطيل أنظمتها".

فوفقًا لهذا النص يمكن معاقبة موزع شبكة الإنترنت بالحبس، لكن هذا النص قد ورد بصيغة عامة، ويستوي في العقاب أن يكون الفاعل أو الشريك من مستخدمي شبكة الإنترنت أو من الوسطاء في توزيع هذه الخدمة، والنص العقابي الوحيد في المشروع والذي وردت فيه الإشارة لموزع الخدمة، باعتبارها صفة تمثل ظرفًا مشددًا للعقوبة، هو نص المادة (30) المتعلقة ببعض الأفعال التي تمثل انتهاكًا للحماية الواجبة لنظام التجارة الإلكترونية، فقد ورد: "مع عدم الإخلال بأي عقوبة أخرى أشد،

يعاقب بالحبس كل من أذاع، أو سهل إذاعة، أو استعمل ولو في غير علانية، محررًا أو توقيعًا إلكترونيًا، أو فض شفرة دون مسوغ قانوني، أو دون موافقة صاحب الشأن، وتكون العقوبة الحبس مدة لا تقل عن سنتين إذا كان مرتكب الأفعال المشار إليها بالفقرة الأولى من كان أمينًا على المحرر أو الموقع أو التوقيع الإلكتروني بمقتضى صناعته أو وظيفته أو كان من العاملين لديه"..

ونجد أن هذا النص شدد العقوبة على موزع خدمة شبكة الإنترنت والعاملين لديه إذا كان أمينًا على المحرر أو التوقيع الإلكتروني وقام بإذاعته أو فض شفرته، أو سهل ذلك بدون مبرر قانوني وبدون موافقة صاحب الشأن.

6- التشريع الإماراتي:

أورد المشرع الإماراتي جريمة نشر شهادة تصديق إلكتروني مزورة وفقًا لنص المادة (25) من القانون الاتحادي في شأن التجارة والمعاملات الإلكترونية رقم 1 لسنة 2006 القاضي نصها بأنه: " لا يجوز لأي شخص أن ينشر شهادة مصادقة إلكترونية تشير إلى مزود خدمات تصديق مدرج اسمه في هذه الشهادة إذا كان الشخص يعلم أن:

أ) مزود خدمات التصديق المدرج اسمه في هذه الشهادة لم يصدرها.

ب) الموقع المدرج اسمه في الشهادة لم يقبلها.

ج) هذه الشهادة قد ألغيت أو أوقفت، إلا إذا كان ذلك النشر بغرض التحقق من توقيع إلكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء".

ويتمثل الركن المادي لهذه الجريمة التي يرتكبها الجاني عن طريق

وسيلة إلكترونية، في صورة من ثلاث وهي[1]:

1) الصورة الأولى: يقوم الجاني بنشر أو استخدام أو استعمال شهادة تصديق إلكتروني مدعى صدورها باسم مزود خدمات تصديق معين في الوقت الذي لم تصدر عنه، ويتحقق السلوك الإجرامي بالنشر عن طريق رسالة عبر البريد الإلكتروني، أو إذاعة بيانات الشهادة شفاهة أو عن طريق استخدام الشهادة ذاتها[2].

2) الصورة الثانية: استعمال الجاني لشهادة تصديق إلكتروني رفض الموقع والمدرج اسمه فيها قبولها لأي سبب كان[3].

3) الصورة الثالثة: استعمال الجاني شهادة تصديق ملغاة أو موقوفة مؤقتًا، إلا إذا كان الاستعمال هدفه الاستيثاق من توقيع إلكتروني أو رقمي صدر قبل قرار الوقف أو الإلغاء.

وتقوم الجريمة بمجرد الاستخدام ولو لم يحقق الجاني الغرض المنشود من هذا الاستخدام، فالسلوك الإجرامي معاقب عليه بصفة مجردة بصرف النظر عن النتائج، ويستهدف ذلك حماية الغير حسن النية الذي تعامل مع الجاني مستخدم الشهادة ولم يكن يعلم أنها ملغاة أو موقوفة[4].

ويتمثل الركن المعنوي في هذه الجريمة العمدية في القصد الجنائي العام بعنصريه العلم والإرادة، ومع ذلك فقد أورد المشرع سبب إباحةٍ بالنسبة

---

(1) د.عبد الفتاح بيومي حجازي، التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، 2006، ص 185.

(2) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية العربية، مرجع سابق، ص 267.

(3) د. خالد محمد المهيري، النظام القانوني للتجارة الإلكترونية في دولة الإمارات العربية المتحدة، مرجع سابق، ص 449.

(4) د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، مرجع سابق، ص 176.

لمـن يستعمل شهادة تصديق إلكتروني ملغاة أو موقوفة، متى كان يقصد من النشر التحقـق مـن توقيع إلكتروني أو رقمي تم استعماله قبل الإيقاف أو الإلغاء[1].

وتكتمل الجريمة بتوافر ركنيها المادي والمعنوي، وتطبق العقوبة القانونية وفقـا لـنص المـادة (26) من القانون وهي الحبس مدة لا تقل عن سنة، والغرامـة التـي لا تقـل عـن خمسـين ألـف درهم ولا تزيد على مائتين وخمسين ألف درهم، أو بواحدة من هاتين العقوبتين.

كما أن المادة (29) من القانون ذاته تعاقب بالحبس مدة لا تزيد على ستة أشهر، وبالغرامـة التي لا تزيد على مائة ألف درهم، أو بإحدى هاتين العقوبتين: كل من ارتكب فعلا يشكل جريمة بموجب التشريعات النافذة باستخدام وسيلة إلكترونية، وفي حالة خضوع الفعـل المـؤثم للعقـاب الوارد في المادتين (26)، (29) من القانون في الوقت ذاتـه، يطبق على المتهم الوصف الأشـد وهـو المنصوص عليه في المادة (26) حيث يزداد الحد الأقصى للحبس، كما يرتفع الحد الأقصى للغرامة.

وفي النهاية فإن المسئولية الجنائية لمقدمي الخدمات الوسيطة عـن جـرائم شـبكة الإنترنـت، وخصوصًا التي تشكل اعتداءً على أطراف التجـارة الإلكترونيـة عـبر شـبكة الإنترنـت، لا يجـب أن تقوم إلا في ضوء القواعد العامة للقانون الجنائي[2]، خصوصًا أن القول بافتراض المسئولية يتعـارض مع المبادئ الدستورية والقانونية العامة في أغلب الـدول، ومنهـا فرنسـا ومصرـ ودولـة الإمـارات العربية المتحدة، وبصفة خاصة مبدأ المسئولية الشخصية، ومبدأ المساواة

(1) د. عبد الفتاح بيومي حجازي، التجارة الإلكترونية العربية، مرجع سابق، ص 268.

(2) Ter Kah Leng, New Laws On E,Commerce" Singapore, Computer Law & Security Report Vol. 15 No. 1 1999.

بين المواطنين أمام القانون، ويلزم أن يتدخل المشرع في البلدان العربية بنصوص واضحة تحدد مجال المسئولية الجنائية عن الجرائم المعلوماتية عمومًا، وعن الجرائم المتعلقة بالتجارة الإلكترونية على وجه الخصوص.



الفصل الرابع

الجرائم الواقعة على الملكية الفكرية والحقوق المجاورة المتصلة بالتجارة الإلكترونية

تمهيد وتقسيم:

الملكية الفكرية هي ثمرة الإبداع والاختراع البشري الفكري، وهي أية ملكية تعتبر فكرية في طبيعتها وجديرة بالحماية، وهذا التعبير الموسع يشمل إبداع الذهن الإنساني في صوره المختلفة شاملا الاختراعات العلمية التكنولوجية، والإنتاج الأدبي أو الفني، والعلامات التجارية، وأدوات التعريف التجارية، والرسوم والنماذج الصناعية، والبيانات الجغرافية.

وتمثل الملكية الفكرية حقوق الملكية المتعلقة بالأمور المعنوية، وهي تعمل على تقديم وسائل دعم التقدم من خلال حماية الحقوق فيما يتعلق بالإبداعات العقلية الجديدة إلى جانب تشجيع المعاملات التجارية، كما تعمل الملكية الفكرية أيضًا على تعزيز تلبية حاجة المستهلك من خلال تنظيم بعض أوجه الممارسات التجارية، ويتم استخدام الملكية الفكرية أساسًا كأداة للأعمال التجارية، بينما تقر أيضًا بعض القيم المعنوية بالنسبة للأعمال الإبداعية.

وحقوق الملكية الفكرية هي أساسًا الحقوق المجسدة في المادة (27) من الإعلان العالمي لحقوق الإنسان[1]، والتي تنص على أنه: " لكل فرد الحق في أن يشترك اشتراكًا حرًا في حياة المجتمع الثقافية، وفي الاستمتاع بالفنون والمساهمة في التقدم العلمي والاستفادة من نتائجه، ولكل فرد الحق في حماية المصالح الأدبية والمادية المترتبة على إنتاجه العلمي أو الأدبي أو الفني".

(1) اعتمدته الأمم المتحدة سنة 1948.

وهي مجموعة من الحقوق تكفلها القوانين الوطنية والاتفاقيات الدولية للمؤلفين المخترعين، وأصحاب الإبداعات الذهنية المختلفة، وتوفر لهم حماية قانونية ضد اعتداءات الغير على إنتاجهم الفكري[1].

ومصطلح الملكية الفكرية هو تعبير إطاري عام يشمل نوعين أساسيين من الملكية هما:

1) حق المؤلف والحقوق المجاورة، والتي تشمل مجموعة واسعة من المصنفات الأدبية والفنية، ويضاف إليها الأداء العلني، ومنتجو التسجيلات الصوتية، وهيئات البث الإذاعي.

2) الملكية الصناعية والتي تشمل الاختراعات الجديدة في مجال العلوم والعلامات التجارية، وعلامات الخدمة، والرسوم والنماذج الصناعية، والبيانات الجغرافية، والأسماء التجارية، والحماية ضد المنافسة غير المشروعة.

وقد أثرت تقنية المعلومات بشكل فاعل على مختلف قواعد النظام القانوني، وخصوصًا في حقل الملكية الفكرية، وتحديدًا فيما يتصل بتوفير الحماية الجنائية للمصنفات الجديدة التي أفرزتها ثورة المعلومات والتقدم العلمي في حقلي الكمبيوتر والاتصالات، بسبب ما أتاحته التقنية من سهولة الاعتداء عليها[2]، وبظهور شبكة الإنترنت بدأ الفقه يفرق بين نوعين من الحقوق، الأول التقليدي (مادي ومعنوي)، والثاني الحقوق الرقمية.

وتتشابك الأهمية فيما بين الملكية الفكرية والتجارة الإلكترونية، ويرجع ذلك إلى أسباب عدة، فالتجارة الإلكترونية تتطلب أكثر من النظم التجارية

(1) فاروق علي الحفناوي، قانون البرمجيات، دار الكتاب الحديث، 2001، ص 65.

(2) David L. Hayes, Advanced Copyright Issues On The Internet, Part VIII, Computer Law & Security Report Vol. 18 No. 1, 2002.

الأخرى، بيع منتجات وخدمات قائمة على الملكية الفكرية، كالاتجار في الموسيقى والرسوم والصور وبرامج الحاسوب والتصاميم والمواد التدريبية والنظم وغيرها بواسطة التجارة الإلكترونية، وتمثل الملكية الفكرية في تلك الحالة المكون الأساسي في المعاملة، ومن ثم تحتاج إلى الحماية باستعمال وسائل التقنية والقوانين، حتى لا تتعرض للسرقة والقرصنة، بما قد يؤدي إلى انهيار المشروع التجاري بأكمله.

وتعمل التجارة الإلكترونية بفضل الملكية الفكرية، فالنظم التي تقوم عليها التجارة الإلكترونية هي جوانب في الملكية الفكرية، وغالبًا ما تكون محمية بموجب قوانين الملكية الفكرية، كبرامج الحاسوب مثلا والشبكات والتصميمات والرقائق الحاسوبية والموجهات والمحولات وواجهات المستخدمين وما إلى ذلك، وتعد العلامات التجارية جزءًا أساسيًا من مشروعات التجارة الإلكترونية، كما أن استعمال العلامات وتعريف المستهلك على المنتج والسمعة التجارية عناصر أساسية في المشروعات التجارية القائمة على وسائل الاتصال الحديثة، ومحمية بموجب العلامات التجارية وقانون المنافسة غير المشروعة.

وتقوم مشروعات التجارة الإلكترونية والمشروعات التجارية المتصلة بشبكة الإنترنت على ترخيص المنتجات أو البراءات، نظرًا لاستعمال تقنيات مختلفة ومتعددة لإبداع بعض المنتجات.

وتعد من الناحية القانونية المصنفات المعلوماتية التي تنتمي إلى بيئة الكمبيوتر، كالبرمجيات وقواعد البيانات[1] وشبكات المعلومات، وأسماء

(1) ومناط حماية قواعد البيانات بوجه عام هو الابتكار كما عبرت عنه الاتفاقيات في هذا الحقل، فالمادة 2/10 من اتفاقية تربس نصت على أنه: "تتمتع بالحماية البيانات المجمعة أو المواد الأخرى، سواء أكانت في شكل مقروء آليًا أو أي شكل آخر =

الحقول أو المجالات، وعناوين البريد الإلكتروني، وقواعد البيانات والتي ارتبطت بشبكة الإنترنت وكانت محصلة الدمج بين وسائل الحاسوبية والاتصال، تثير مسألة الحاجة إلى الحماية القانونية[1]، وتحديدًا فيما يتعلق بالدخول إليها واسترجاع البيانات منها، والتبادل المتعلق بمحتواها، وهو تطور لمفهوم قواعد البيانات الذي كان سائدًا قبل انتشار الشبكات.

ونحن نرى أن المصنف الرقمي يشمل كافة المصنفات المتقدمة، فبرنامج الكمبيوتر من حيث البناء والأداء مصنف رقمي، وكذلك قاعدة البيانات من حيث ترتيبها وتبويبها، وأي مصنف إبداعي ينتمي إلى بيئة تقنية المعلومات يعد مصنفًا رقميًا.

وبما أن موضوع الملكية الفكرية يتم تقسيمه إلى قسمين: حقوق المؤلف وحقوق الملكية الصناعية، فسوف نتناول المصنف الرقمي باعتباره الصورة الحديثة لحقوق المؤلف في المجال المعلوماتي، والحماية الجنائية الدولية والوطنية لها، ثم مسألة حماية أسماء حقول شبكة الإنترنت، باعتبارها صورة حديثة للعلامات التجارية كل في مبحث كالآتي.

المبحث الأول: الحماية الجنائية للمصنف الرقمي

المبحث الثاني: الحماية الجنائية الدولية والوطنية لحقوق مؤلف برامج الحاسب الآلي

المبحث الثالث: الاعتداء على العلامة التجارية عبر شبكة الإنترنت

= إذا كانت تشكل خلقًا فكريًا نتيجة انتقاء وترتيب محتواها"، كما نصت المادة (5) من الاتفاقية العالمية للملكية الفكرية لسنة 1996 غير النافذة على أنه: "تتمتع مجموعات البيانات أو المواد الأخرى بالحماية بصفتها هذه أيًا كان شكلها إذا كانت تعتبر ابتكارات فكرية بسبب محتواها أو ترتيبها".

(1) قواعد البيانات هي تجميع مميز للبيانات يتوافر فيه عنصر الابتكار أو الترتيب أو التبويب عبر مجهود شخصي بأي لغة أو رمز، ويكون مخزنًا بواسطة الحاسوب، ويمكن استرجاعه بواسطته أيضًا.

المبحث الأول

الحماية الجنائية للمصنف الرقمي

تثار بين حين وآخر الكثير من قضايا حقوق المؤلفين واستيلاء الغير على مصنفاتهم أو القيام بتعديلها أو الأخذ منها، وظلت ساحة القضاء ميدانًا لكل النزاعات بين المؤلف وبين المستفيدين من حقوقه الأدبية والمالية أو من استولوا عليها.

ويفرض القانون حماية المصنف أيًا كان شكله، فتشمل الحماية نسبة المصنف إلى صاحبه كضرورة، ولا تمتد الحماية لتشمل مجرد الأفكار إذ تظل في منأى عن حماية القانون.

وقبل الحديث عن المصنف المشمول بالحماية سنوضح من هو المؤلف صاحب هذا المصنف وفقا لما ورد في القانون.

المؤلف - من حيث المبدأ - هو الشخص الذي خلق أو ابتكر المصنف، وهو صاحب الحق في حقوق المؤلف، فإذا اشترك عدة أشخاص في ابتكار وخلق المصنف كانوا جميعًا أصحاب الحق في حقوق المؤلف[1].

وقد عرف قانون حقوق المؤلف والحقوق المجاورة لدولة الإمارات العربية المتحدة رقم 7 لسنة 2002 المؤلف بأنه الشخص الذي يبتكر المصنف، ويعد مؤلفًا للمصنف من يذكر اسمه عليه، أو ينسب إليه عند نشره باعتباره مؤلفًا له، ما لم يقم الدليل على غير ذلك.

كما يعتبر مؤلفًا للمصنف من ينشره بدون اسم أو باسم مستعار أو بأية طريقة أخرى، بشرط ألا يقوم شك في معرفة حقيقة شخصية المؤلف، فإذا

(1) د. محمود السيد عبد المعطي خيال، الإنترنت وبعض الجوانب القانونية، مرجع سابق، ص 44.

قام الشك اعتبر ناشر أو منتج المصنف - سواء أكان شخصا طبيعيًّا أم اعتباريًّا - نائبًا عن المؤلف في مباشرة حقوقه إلى أن يتم التعرف على حقيقة شخصية المؤلف.

والمؤلف قد يكون شخصا طبيعيًّا أو اعتباريًّا، وقد يكون مجموعة مكونة من أشخاص طبيعيين أو اعتباريين، وحق المؤلف لا يخرج عن كونه حقًّا استئثاريًّا يمنحه القانون لمؤلف أي مصنف للكشف عنه كابتكار له، أو استنساخه، أو توزيعه أو نشره على الجمهور بأي طريقة أو وسيلة، وكذلك الإذن للغير باستعماله على وجه محدد[1].

وحقوق المؤلف على مصنفه تنقسم إلى قسمين: حقوق أدبية، وأخرى مالية، والحقوق الأدبية نصت عليها المادة [5] من القانون الإماراتي وهي كالتالي:

أ) الحق في تقرير نشر المصنف لأول مرة، وهو ما يسمى بحق النشر، فللمؤلف وحده الحق في تحديد لحظة إصدار مصنفه واتصاله بالجمهور، فإذا ما نشر هذا المصنف بدون إذنه عدّ ذلك عملا غير مشروع.

ب) الحق في نسبة المصنف إليه، وهو ما يسمى بحق الأبوة، فللمؤلف الحق في نسبة المصنف إليه سواء باسمه أو باسم مستعار، ويظل محتفظًا بأبوته لهذا المصنف.

ج) الحق في الاعتراض على أي تعديل للمصنف إذا كان في التعديل تشويه أو تحريف للمصنف أو إضرار بمكانة المؤلف، ويسمى بالحق في سلامة المصنف، أو احترام المصنف، فللمؤلف وحده الحق في دفع أي اعتداء على مصنفه، فلا يجوز إبداء أي اعتراض أو تعديل

(1) **عفيفي كامل عفيفي، جرائم الكمبيوتر، مرجع سابق، ص 61.**

عليه إلا بإذن من المؤلف، فهو الذي يملك إبداء أي تعديل على مصنفه لتحسينه وتحديثه.

د) الحق في سحب مصنفه من التداول، وهذا ما يطلق عليه حق الندم، فهو الوحيد الذي يستطيع إذا ما طرأت أية أسباب أن يسحب مصنفه من التداول، وأن يوقف نشره أو عرضه أو إذاعته، وقرر القانون أن يباشر المؤلف هذا الحق عن طريق المحكمة المختصة، مع إلزامه بأن يدفع تعويضًا عادلا مقدمًا إلى من آلت إليه حقوق الاستغلال المالي، وذلك في الأجل الذي تحدده المحكمة وقبل تنفيذ الحكم بالسحب، وإلا زال كل أثر للحكم.

أما الحقوق المالية فتتمثل في العائد المادي من هذا المصنف والذي هو نتيجة جهد هذا المؤلف، وبالتالي من حقه الحصول على مقابل لثمرة فكره، وقد أعطى القانون في المادة (10) للمؤلف وخلفه أن يتقاضى المقابل النقدي أو العيني نظير نقله حقًّا أو أكثر من حقوق الاستغلال المالي للمصنف إلى الغير، كما نص القانون على حماية الحقوق المالية للمؤلف مدة حياته وخمسين سنة تبدأ من أول السنة الميلادية التالية لسنة وفاته، (المادة (20) من القانون).

وقد عرف قانون حقوق المؤلف والحقوق المجاورة الإماراتي المصنف بأنه كل تأليف مبتكر في مجال الآداب أو الفنون أو العلوم، أيًا كان نوعه أو طريقة التعبير عنه أو أهميته أو الغرض منه.

فالمصنف هو كل إنتاج ذهني أو فكري أيًا كانت الصورة المادية التي يبدو فيها، بغض النظر عن نوعه وأهميته، أو الغرض من وضعه، أو طريقة التعبير عنه[1].

(1) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، مرجع سابق، ص 77.

والمصنف على هذا الأساس لا يكفي أن يكون مجرد فكرة فقط، وإنما يجب أن تكون هذه الفكرة مبتكرة، وموضوعة في إطار مادي ملموس تبرز فيه إلى الوجود، وبالتالي تشكل المصنف الذي يجب أن يكون معدًا للنشر، لا مجرد فكرة يعوزها الإطار الذي تتجسم فيه، فيجب إذن أن يكون مظهر التعبير عن الفكرة قد بلغ الغاية من الوضع المستقر[1].

والمصنف في موضوعه قد تشمله الحماية من حيث التأليف أو التصنيف، وكذلك قد تشمله الحماية من حيث كونه مصنفًا، أو من حيث كونه علامة مسجلة، أو من حيث جدة اختراعه وبالتالي يلزم أن تلحقه براءة اختراع[2]، أو من حيث الأسرار التجارية، وأيضًا قد تشمله الحماية لكونه برمجية حاسوب.

وتعرف المادة (138) من القانون المصري رقم 82 لسنة 2002 بشأن حماية حقوق الملكية الفكرية المصنف بأنه: " كل عمل مبتكر أدبي أو فني أو علمي، أيًا كان نوعه أو طريقة التعبير عنه أو أهميته أو الغرض من تصنيفه". والمصنف الذي يحميه القانون لا يقتصر على نوع معين أو على طريقة تعبير معينة، فأيًا كانت طريقة التعبير يكون محميًا، كما أن الغرض من المصنف لا يهم أيضًا في مجال الحماية، ويميز الفقه بين ثلاثة أنواع من المصنفات: هي الأدبية، والفنية، والعلمية.

(1) خاطر لطفي، الموسوعة الشاملة في قوانين حماية حق المؤلف والرقابة على المصنفات الفنية، 1994، ص 21.

(2) Marshall J. Wech، International protection of intellectual property P. 1، Texas intellectual property journal, the university of Texas school of law, [1، Twx. Intel. Prop، 1، j، 44] 1993 , Available online at: http://www.utexas.edu/law/journals/tipilj/vollissI/welch.htm.SECI

والمصنف يجب أن يشتمل على عنصرين: الأول شكلي، والثاني موضوعي، ويقصد بالعنصر الشكلي هو أن يكون المصنف ثابتًا على دعامة معينة تسهل عملية وصوله إلى الغير، وبدون هذا الشكل لا يتوافر للمصنف أحد عناصره، ويصبح مجرد فكرة لا تشملها الحماية بقانون حق المؤلف، ويقصد بالعنصر الموضوعي أن يكون المصنف مبتكرًا، أي أن شخصية المؤلف تظهر بوضوح في مصنفه.

والشكل الذي يعبر به عن المصنف لا يشترط أن يكون بطريقة معينة، فالحماية تشمل المصنف أيًا كانت طريقة التعبير عنه، وأيًا كان الهدف أو الغرض من هذا المصنف، كما أن قيمة المصنف وأهميته ليست محل اعتبار عند تقرير الحماية[1]، وهو ما سوف نتعرض له ولكن بعد أن نبين أركان المصنف الجديرة بالحماية، ونتحدث عن نسبة المصنف إلى مؤلفه وفقا لما يلي:

أولا - التجريم وفقا لأركان المصنف:

تتعلق هذه المسألة بمدى إمكانية امتداد الحماية الجنائية التي يفرضها القانون إلى أي من العناصر الثلاثة المكونة للركن الموضوعي في المصنف، بمعنى أن يكون الاعتداء موجهًا إلى أحد هذه العناصر: عنوان المصنف، أو موضوعه، أو اسم المؤلف، وليس إلى المصنف ككل.

ويربط الفقه في بحث الاعتداء على حق المؤلف والملكية الفكرية، باعتبار أن الحقوق الذهنية أحد عنصري نظرية الحق، فيقتصر على مجرد رصد مجموعة الحقوق التي يتشكل منها حق المؤلف، وتكون الحماية الجنائية مقررة للمصلحة المالية للمؤلف على مصنفه، في حين أن الاعتداء

(1) P. Sérielle: La propriété littéraire et droits voisins , Ed Dalloz, 1992, P. 11.

يتناول المصنف ذاته الذي وضعه مؤلفه، وكنتيجة لهذا الخلط رفضت فكرة إمكانية تجريم الاعتداء الجزئي على المصنف، وإن كان العمل جرى على شمول الحماية الجنائية لمادة المصنف وهي أحد أركانه.

وتبعًا لذلك فإنه يقبل في القانون أن تمتد الحماية القانونية إلى الأركان، كعنوان المصنف[1] واسم المؤلف لكونها أمورًا لازمة في تكوينه، ما دامت كلها داخلة في الطابع الابتكاري للمصنف، وهو أمر أقره المشرع في تشريعات حقوق المؤلف، حيث تضمن القانون المصري رقم 82 لسنة 2002 بشأن حقوق الملكية الفكرية في المادة 140 النص على أنه: "... وتشمل الحماية عنوان المصنف إذا كان مبتكرا"، كما أكد المشرع الفرنسي على حماية عنوان المصنف الأدبي بما قرره في المادة 4 /112 من قانون الملكية الفكرية الفرنسي- من أن عنوان المصنف الأدبي منذ بروزه في شكل أصلي مشمول بالحماية مثل المصنف ذاته.

ثانيًا: نسبة المصنف إلى مؤلفه:

قضت محكمة النقض المصرية في حكم لها بأن "النص في الفقرة الأولى من المادة التاسعة من القانون رقم 1345 سنة 1954 بإصدار قانون حماية حق المؤلف تم إلغاؤه بإصدار قانون حماية الملكية الفكرية رقم 82 لسنة 2002، على أن للمؤلف وحده الحق في أن ينسب إليه مصنفه، وفي أن يدفع أي اعتداء على هذا الحق... دل على أن للمؤلف الحق دائمًا في أن يكتب اسمه على كل نسخة من نسخ المصنف الذي ينشره بنفسه أو بواسطة غيره، وفي جميع الإعلانات عن هذا المصنف بغير حاجة إلى إبرام اتفاق

(1) د. أسامة عبد الله قايد، الحماية الجنائية لحق المؤلف، الطبعة الأولى، دار النهضة العربية، 1991، ص 42.

مع الغير على ذلك[1].

كما يشمل مدلول نسبة المصنف إلى مؤلفه أنه: "للمؤلف وحده الحق في أن ينسب إليه مصنفه، وله حق استغلاله ماليًا، ولا يجوز لغيره مباشرة هذا الحق دون إذن سابق منه أو ممن يخلفه، وله أن ينزل عن حق الاستغلال هذا بما يشمله مضمونه من الحق في النشر"[2]، وفي حال قيام المؤلف بعدم نشر مصنفه لسبب أو لآخر، ففي مثل هذه الحالة لا يكون للغير تناول المصنف المتروك أو المهمل؛ إذ يظل المصنف المتروك في كافة صوره الموضعية منسوبًا إلى المؤلف الأصلي وحده، وله الحق في الدفاع عنه[3].

وقد توسع القانون المصري الجديد رقم 82 لسنة 2002 ليأخذ شكلا مباشرًا كما هو مقرر في المادة (143) التي تنص على أنه: "يتمتع المؤلف وخلفه العام على المصنف بحقوق أبدية غير قابلة للتقادم أو للتنازل عنها، وتشمل هذه الحقوق ما يلي: الحق في إتاحة المصنف للجمهور لأول مرة، والحق في نسبة المصنف إلى مؤلفه، وأخيرًا الحق في منع تعديل المصنف تعديلا يعتبره المؤلف تشويهًا أو تحريفًا له، ولا يعد التعديل في مجال الترجمة اعتداءً إلا إذا أغفل المترجم الإشارة إلى مواطن الحذف أو التغيير، أو أساء بعمله لسمعة المؤلف ومكانته"[4]، كما تنص المادة (145) من القانون ذاته على أنه: "يقع باطلا بطلانًا مطلقًا كل تصرف يرد على أي من

---

(1) نقض مصري رقم 1352 لسنة 53 ق، جلسة 1987/1/7.
(2) طعن مدني مصري رقم 1568 لسنة 54 ق، جلسة 1988/11/3.
(3) د. عبد الحفيظ بالقاضي، مفهوم حق المؤلف وحدود حمايته جنائيًا، رسالة دكتوراه، كلية الحقوق، الرباط، 1995، دار الأمان، المغرب، ص 307.
(4) فيما يتعلق بالفقرة الأخيرة أعلاه يراجع نص المادة (148) من هذا القانون، وفيما يتعلق بالحقوق الأبدية لفناني الأداء انظر نص المادة (155) من هذا القانون.

الحقوق الأدبية المنصوص عليها في المادتين (143،144) من هذا القانون.

وفي المعنى ذاته نصت المادة الخامسة من القانون الإماراتي الاتحادي رقم 2002/7 بشأن حقوق المؤلف والحقوق المجاورة على أنه: (يتمتع المؤلف وخلفه العام بحقوق أدبية غير قابلة للتقادم أو التنازل عن المصنف، وتشمل هذه الحقوق ما يلي: الحق في تقرير نشر المصنف لأول مرة، الحق في نسبة المصنف إليه، الحق في الاعتراض على أي تعديل للمصنف إذا كان في التعديل تشويه أو تحريف للمصنف أو إضرار بمكانة المؤلف، الحق في سحب مصنفه من التداول إذا طرأت أسباب جدية تبرر ذلك، ويباشر هذا الحق عن طريق المحكمة المختصة، مع إلزامه بأن يدفع تعويضًا عادلا مقدمًا إلى من آلت إليه حقوق الاستغلال المالي، وذلك في الأجل الذي تحدده المحكمة وقبل تنفيذ الحكم بالسحب، وإلا زال كل أثر للحكم).

وعليه فكل عدوان على أي من عناصر المصنف الثلاثة، وهو عدوان جزئي، إنما يعتبر عدوانًا على المصنف ككل، ويجوز لمالك المصنف اتخاذ الإجراءات القانونية ضد مرتكب هذه الجريمة لكونه قد نسب إلى نفسه المصنف المذكور أو اعتدى على حقوق المؤلف بصورة أخرى، فضلا عن اللجوء إلى القضاء المدني للمطالبة بالتعويض عما ارتكبه الجاني من خطأ، وما سببه من ضرر بحقوق المؤلف التي يحميها القانون.

ويكون استخدام عنوان مصنف مادي بوضعه على برمجية، ليكون عنوانًا لها، إنما يعد مرتكبا لجريمة الاعتداء على حقوق الملكية الفكرية بنسبة المصنف لنفسه، ومثاله من قام بوضع عنوان مصنف موجود على كتاب أو موسوعة أو مجموعة صور أو شريط فيديو، وطرحه في التداول في برمجية حاسوب أو عبر شبكة الإنترنت.

ثالثًا: برامج الحاسب الآلي وطريقة التعبير:

يشترط قانون حق المؤلف والحقوق المجاورة الإماراتي رقم 7 لسنة 2002, وقانون حماية الملكية الفكرية المصري رقم 82 لسنة 2002 لحماية المصنف الفكري أن يتم التعبير عنه أيًا كانت طريقة التعبير، ونصًا على أنه لا يهم طريقة التعبير عن المصنف، فليس معنى ذلك تجاهل التعبير عن المصنف، فالتعبير هو الرداء الذي يحمي الفكرة ويدخلها في نطاق الحماية بقانون حق المؤلف، فالكلمات هي رداء المصنفات الأدبية، والصوت هو رداء المصنفات الموسيقية، والشكل هو رداء المصنفات الفنية[1]، فالعبرة بخروج الفكرة من عالمها المجرد إلى العالم المحسوس.

فنوع الركيزة أو الدعامة التي تحوي المصنف لا يهم في مجال تقرير الحماية بقانون حق المؤلف، فوسائل التعبير متعددة يمكن أن تكون كتابة، أو فيلمًا، أو صورة ضوئية، أو أسطوانة ممغنطة، وذلك بالطبع حسب طبيعة المصنف، وترتيبًا على ذلك تم إقرار حماية المصنفات التي ظهرت على ركائز جديدة، مثل الأعمال السينمائية، بل إن الحماية تكون واجبة للمصنفات التي يتم التعبير عنها شفاهة دون تثبيتها على ركيزة مادية[2].

وفيما يتعلق ببرامج الحاسب الآلي نجد أن هناك بعض التشريعات العربية لم تنص على إدراج برامج الحاسب الآلي ضمن المصنفات الفكرية المعروفة، فهي تعتبرها من المصنفات الفكرية، لكنها منفصلة أو مستقلة عن المصنفات المعروفة بواسطة القانون، وعلى سبيل المثال القانون السعودي رقم 11 الصادر في 17 ديسمبر 1989، والقانون الأردني رقم 22 الصادر

(1) A l Luca: Dorit auteur et numèrique, Ed. litec , 1998 , P 24.

(2) د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، رسالة دكتوراه، جامعة عين شمس، 1992، ص 201.

في ديسمبر 1992، والقانون التونسي رقم 36 - 94 الصادر في 24 فبراير 1994، هذه التشريعات اعتبرت برامج الحاسب الآلي مصنفًا فكريًا يخضع للحماية بقانون حق المؤلف، لكنه مصنف مستقل عن المصنفات الفكرية الأخرى المعروفة.

وقد نصت بعض القوانين العربية الأخرى على إدخال برامج الحاسب الآلي ضمن المصنفات الأدبية، فالقانون الاتحادي لدولة الإمارات العربية المتحدة نص على حماية المصنفات الفكرية بقانون حق المؤلف أيًا كانت قيمتها أو أهميتها أو طريقة التعبير عنها، وأدخل برامج الحاسب الآلي ضمن هذه المصنفات المشمولة بالحماية[1].

---

(1) المادة (2) من القانون الاتحادي لدولة الإمارات العربية المتحدة رقم 40 لسنة 1992 بشأن حماية المصنفات الفكرية بقانون حق المؤلف والتي تنص على أن: (يتمتع بالحماية المقررة في هذا القانون مؤلفو المصنفات وأصحاب الحقوق المجاورة، إذا وقع الاعتداء على حقوقهم داخل الدولة، وبوجه خاص المصنفات الآتية:
1) الكتب والكتيبات والمقالات وغيرها من المصنفات الفكرية.
2) برامج الحاسب وتطبيقاتها، وقواعد البيانات، وما يماثلها من مصنفات تحدد بقرار من الوزير.
3) المحاضرات والخطب والمواعظ والمصنفات الأخرى التي لها طبيعة مماثلة.
4) المصنفات التمثيلية والمصنفات التمثيلية الموسيقية والتمثيل الصامت.
5) المصنفات الموسيقية المصحوبة أو غير المصحوبة بكلمات.
6) المصنفات السمعية أو البصرية أو السمعية البصرية.
7) مصنفات العمارة والرسوم والمخططات الهندسية.
8) مصنفات الرسوم بالخطوط أو بالألوان، والنحت، والنقش، والطباعة على الحجر، وعلى الأقمشة، وعلى الخشب، وعلى المعادن وأية مصنفات مماثلة في مجال الفنون الجميلة.
9) المصنفات الفوتوغرافية وما يماثلها. =

كما أن المشرع المصري قد نص على حماية برامج الحاسب الآلي بقانون حق المؤلف على أساس أنها مصنف فكري مستقل عن المصنفات الفكرية الأخرى المحمية بواسطة القانون[1].

= 10) مصنفات الفن التطبيقي والتشكيلي.
11) الصور التوضيحية، والخرائط الجغرافية، والرسومات التخطيطية، والمصنفات ثلاثية الأبعاد المتعلقة بالجغرافيا أو الطبوغرافيا أو التصميمات المعمارية وغيرها.
12) المصنفات المشتقة، دون الإخلال بالحماية المقررة للمصنفات التي اشتقت منها، وتشمل الحماية عنوان المصنف إذا كان مبتكرًا، كما تشمل الفكرة المبتكرة المكتوبة للبرنامج الإذاعي).

(1) المادة 140 من القانون المصري رقم 82 لسنة 2002 بشأن حماية حقوق الملكية الفكرية تنص على أن: (تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية، وبوجه خاص المصنفات الآتية:
1- الكتب والكتيبات والمقالات والنشرات وغيرها من المصنفات المكتوبة.
2- برامج الحاسب الآلي.
3- قواعد البيانات سواء كانت مقروءة من الحاسب الآلي أو من غيره.
4- المحاضرات والخطب والمواعظ وأية مصنفات شفوية أخرى إذا كانت مسجلة.
5- المصنفات التمثيلية والتمثيليات الموسيقية والتمثيل الصامت (البانتوميم).
6- المصنفات الموسيقية المقترنة بالألفاظ أو غير المقترنة بها.
7- المصنفات السمعية البصرية.
8 - مصنفات العمارة.
9- مصنفات الرسم بالخطوط أو بالألوان، والنحت، والطباعة على الحجر وعلى الأقمشة، وأية مصنفات مماثلة في مجال الفنون الجميلة.
10- المصنفات الفوتوغرافية وما يماثلها.
11- مصنفات الفن التطبيقي والتشكيلي.
12- الصور التوضيحية والخرائط الجغرافية والرسومات التخطيطية (الإسكتشات) والمصنفات الثلاثية الأبعاد المتعلقة بالجغرافيا أو الطبوغرافيا أو التصميمات=

وبرامج الحاسب الآلي تخضع للحماية بقانون حق المؤلف، أيًا كانت طريقة التعبير عنها، فالحماية بقانون حق المؤلف تمنح استقلالا عن الركيزة التي تنقل العمل، فبرامج الحاسب الآلي المثبتة على أسطوانة خاصة أو على شريط ممغنط تستفيد من الحماية بحق المؤلف.

ويشترط القانون لبسط حماية حق المؤلف على المصنف أن تكون الركيزة المثبت عليها برامج الحاسب محسوسة ومدركة من الغير، لأن المصنف لا يكون محميًا إلا إذا كان محسوسًا ومدركًا من الغير، ولمعرفة ذلك اتجه البعض إلى التفرقة بين نوعين من البرامج، برامج المصدر وبرامج الهدف، وبرامج المصدر هي البرامج التي يكتبها المعلوماتي بلغة مبرمجة مفهومة للإنسان، ثم يتم بعد ذلك ترجمة هذه البرامج إلى لغة تفهمها الآلة أو يفهمها الجهاز، وهي ما يعرف هنا ببرامج الهدف[1].

فبرامج المصدر لا تثير أية مشكلة فيما يتعلق بمعرفة كونها محسوسة ومدركة من الغير، خاصة وأنها مفهومة من قبل الإنسان، ولكن المشكلة تتعلق ببرامج الهدف التي تكون مفهومة للجهاز فقط وغير موجهة للإنسان

= المعمارية.

13 ـ المصنفات المشتقة، وذلك دون الإخلال بالحماية المقررة للمصنفات التي اشتقت منها، وتشمل الحماية عنوان المصنف إذا كان مبتكرًا.

(1) برامج الحاسب الآلي تكتب بلغة عالية المستوى تسمى لغة المصدر، ولكي يعمل هذا البرنامج على الحاسب لابد من ترجمته إلى اللغة الوحيدة التي تفهمها المكونات المادية للحاسب وهي لغة الآلة، ولهذا يطلق على البرنامج بعد تحويله إليها برنامج الهدف، وقد جرى العمل في عقود البيع الواردة على برامج سابقة الإعداد أن يطرح للبيع برنامج الهدف فقط، أما برنامج المصدر فيحتفظ به المنتج. انظر في هذا الصدد: د.أسامة محمد محيي الدين، مدخل الحاسب الآلي ونظم المعلومات، ج 1، مقدمة الحاسب الآلي، ط 1، دار القلم، دبي، 1990، ص 127.

بطريقة مباشرة[1].

وفي الواقع فإن المشرع الإماراتي والمشرع المصري عندما أدخلا برامج الحاسب الآلي في نطاق الحماية بقانون حق المؤلف لم يتعرضا لمسألة كون البرامج محسوسة ومدركة من الغير أم لا، كما أنهما لم يفرقا بين برامج المصدر وبرامج الهدف، فالبرامج تكون محمية أيًا كانت المرحلة التي تمر بها.

كما أن شرط توجيه الأعمال الذهنية إلى الجمهور حتى تتمتع بالحماية المقررة في القانون سيؤدي إلى استبعاد برامج الحاسب الآلي من نطاق الحماية، على الرغم من أن الحماية بقانون حق المؤلف تمنح لأعمال لم تكن مخصصة للنشر، ولم يكن الهدف أو الغرض منها توجيهها للجمهور كما هو الحال بالنسبة للمذكرات الخاصة أو الشخصية[2].

لذلك يمكننا القول بأن كون برامج الحاسب الآلي موجهة للأجهزة الآلية وليس إلى الإنسان ليس سببًا كافيًا لاستبعادها من نطاق الحماية بقانون حماية حقوق المؤلف، خاصة وأن هذه البرامج يمكن أن تكون مدركة بطريقة مباشرة للإنسان أو بطريقة غير مباشرة عن طريق جهاز الحاسب الآلي، كما هو الوضع تمامًا بالنسبة للأعمال السينمائية والموسيقية التي لا يمكن الحس بها أو إدراكها إلا عن طريق أجهزة معينة، ثم إن المقطوعات الموسيقية لا تصل إلى الجمهور ولا يمكن استيعابها وإدراكها إلا بخبرة ودراية بأصول ما يسمى (النوتة الموسيقية) التي تبدو للإنسان العادي كرموز غير مفهومة".

(1) د. أمين أعزان, الحماية الجنائية للتجارة الإلكترونية, مرجع سابق, ص 318.
(2) د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، مرجع سابق، ص 202.

فإذا كانت المصنفات الفكرية الأخرى كالأدبية منها والفنية يمكن أن تكون محسوسة ومدركة من الغير، وكانت برامج الحاسب الآلي غير موجهة إلى الإنسان، بل موجهة إلى الآلة، فإن العبرة بالنتيجة، والنتيجة تكمن في أن برامج الحاسب الآلي بفضل نقلها على الركائز المادية كظهورها على شاشة الحاسب الآلي يمكن أن تكون مدركة بواسطة الغير[1].

وهذا هو ما اتجه إليه القضاء الفرنسي في أحد أحكامه، حيث ذهبت محكمة باريس الابتدائية في حكم لها إلى أن برامج الحاسب الآلي إذا كانت لا تتجه بشكل مباشر إلى الإنسان، فإن هذا ليس تبريرًا لاستبعادها من نطاق الحماية بقانون المؤلف، فبفضل نقل هذه البرامج على ركائز مادية مثل ظهورها على شاشة الحاسب الآلي أو تسجيلها على الأسطوانات المغنطة، فإنها تصل إلى الإنسان، وليس معنى الاحتياج إلى إنسان على مستوى عال من القدرة على قراءة البرنامج هو استبعادها من نطاق الحماية لعدم إلمام الجمهور بها، فالمقطوعات الموسيقية تكتب بلغة رمزية معقدة لا يفهمها الجميع، ورغم ذلك لم يستبعدها أحد من نطاق الحماية بقانون حق المؤلف[2].

---

(1) د. أمين أعزان, الحماية الجنائية للتجارة الإلكترونية, مرجع سابق, ص 319.

(2) **Si les programmes d'ordinateur ne sont pas immédiatement perceptible par les sens de locus comme le sont les ouvres littéraires ou artistiques, ils sont mimions accessible et inéligibles agace à leur transcription sur divers supports matériels , tells que les écrans où les enregistrements magnétiques , que si. a l'riels, tells que les écrans ou les enregistrements magnétiques, que si. á l'évidence, leur lecture ne est pas à la prote de tous et requière une technicité certaine , cette seule particularité ne est pas de nature à les exclure de la catégorie de ouvres de l'esprit pas plus que n'en sont sexlues.par example.ies compositions musicales qui**

كما أن لجنة الخبراء بالمنظمة العالمية للملكية الفكرية قبلت حماية المصنفات المعبر عنها بشكل غير مقروء إلا بواسطة الآلة، وقد أكدت هذه اللجنة على أنه: "إذ لم نقر حماية المصنفات التي لا يمكن قراءتها أو إيصالها للغير إلا عن طريق الآلة، فإن معنى ذلك هو نهاية الحماية بقانون حق المؤلف، ثم إن السرعة والتطور في مجال المعلوماتية يجعل من الممكن وجود العديد من المصنفات التي لا يمكن إدخالها في النظام المعلوماتي إلا بهذه الطريقة[1]".

رابعًا: قيمة المصنف وأهميته وغرضه:

أسبغ المشرعان الإماراتي والمصري الحماية على المصنف المبتكر أيًا كانت أهميته أو قيمته أو حتى الغرض منه، فالقانون حمى المصنفات كلها دون تمييز بينها بسبب القيمة أو الأهمية، ويستوي أن يكون المصنف طويلا أو قصيرًا، مفيدًا أو غير مفيد، عاديًا أو خطرًا، ثمرة عبقرية أو مجرد نتاج مجهود طويل، فلا يجوز أن نربط الحماية بصفات المصنف، كما أن القضاة عند نظرهم لمدى استحقاق الحماية، لا يجب أن يكون تذوقهم الشخصي للمصنف محل اعتبار لتقرير الحماية من عدمها[2]، وليس معنى ذلك التخلي عن شرط ابتكار البرنامج، فمسألة قيمة المصنف أو أهميته شيء، ومسألة توافر الطابع الابتكاري شيء آخر، كما أن المادة (138) من القانون المصري 2002/82 تشير إلى عدم الاعتداد بالغرض من المصنف حتى

sont. elles aussi. exprimées en un langage code et complexe dont la compréhension immédiate suppose une éducation spécialisée".

Vol TGI paris, 215 Sep 1983. D. 1984 , 77 Note Le Stance.

(1) www.wipo.int

(2) د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، مرجع سابق، ص209.

يتمتع بالحماية المقررة في هذا القانون، فيستوي كون الهدف أو الغرض من المصنف نفعيًّا، أم أن له بعدًا ثقافيًّا آخر، فالمصنف الذي يعد من الفن المطلق أو ما يطلق عليه أحيانًا الفن من أجل الفن خاصة في مجال الصناعة يستحق الحماية، بمعنى آخر لا قيمة ولا تأثير لكون العمل ذا هدف جمالي فقط، أو أن يكون له هدف نفعي[1].

خامسًا: برامج الحاسب الآلي والطابع الابتكاري:

تستلزم نصوص قانون حماية الملكية الفكرية المصري والإماراتي الخاصين بحق المؤلف أن يكون المصنف الفكري مبتكرًا كي يتمتع بالحماية، فتوافر الطابع الابتكاري شرط جوهري للتمتع بالحماية بقانون حق المؤلف.

وفيما يتعلق ببرامج الحاسب الآلي دارت العديد من المناقشات حول مدى توافر الطابع الابتكاري فيها، فهناك من وافق على حماية برامج الحاسب الآلي بقانون حق المؤلف لتوافر عنصر الابتكار، وهناك من أنكر الحماية لهذه البرامج.

ويكون المصنف مبتكرًا إذا كان يعبر عن شخصية مؤلفه ومجهوده الذهني، فالابتكارية تعد معيارًا شخصيًّا يحدد مدى حماية المصنف بقانون حق المؤلف[2]، وفكرة الابتكارية يمكن البحث فيها بطريقة موضوعية وشخصية.

---

(1) ويقول البعض: إن الرسم الذي تم إعداده للدعاية لسلعة معينة يأخذ أو يتمتع بنفس الحماية التي تكون مقررة للوحة فنية أخرى تم إعدادها لمعرض معين أو لوضعها في متحف معين.
في هذا الصدد انظر: د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، مرجع سابق، ص 211.

(2) A l Lucas: Droit d'auteur et numérique: op. cit, no 67 , P. 33.

وتتميز فكرة الابتكارية المطلوب توافرها لإقرار الحماية بقانون حق المؤلف عن فكرة الجدة أو الحداثة المطلوب توافرها لإقرار الحماية بقانون براءة الاختراع، فالجدة تقدر على أساس معيار موضوعي هو مدى توافر الأسبقية من عدمه، بحيث لا نأخذ في الاعتبار شخصية المخترع، أما الابتكارية فإنها تقدر بناءً على معيار شخصي- هو النظر إلى شخصية المؤلف ومدى إضافته للمصنف الذي قام بتأليفه[1].

وتنقسم الابتكارية إلى نوعين، مطلقة تعني قيام شخص بعمل معين وظهرت فيه شخصيته، ونسبية تعني قيام شخص ثان - أو ما يسمى بالمؤلف الثاني - بأداء العمل نفسه مع وضوح شخصيته؛ لأنه لم يقم بتأليف موضوع جديد، بل قام بنفس العمل الذي قام به المؤلف الأول.

وأيًّا كان النوع فكل من الابتكارية المطلقة والنسبية تعطي صاحب العمل الحق في طلب الحماية بقانون حق المؤلف، لكن إذا قام المؤلف الثاني بمجرد نسخ ما قام به المؤلف الأول دون إضافات معينة توضح شخصيته، فإنه في هذه الحالة لا يستفيد من الحماية المقررة في قانون حق المؤلف.

ويجب ملاحظة أن مؤلف العمل ذي الابتكارية النسبية رغم استفادته من الحماية فهذه الأخيرة غير مطلقة، حيث يلتزم بتقديم مقابل لفائدة المؤلف الأصلي للعمل الذي استوحى منه[2].

وللبحث عن مدى توافر الابتكارية يجب تقسيم العمل المراد حمايته إلى ثلاثة أقسام أو إلى ثلاث مراحل: مرحلة اختيار الموضوع، ثم مرحلة

---

(1) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، مرجع سابق، ص8.

(2) د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، مرجع سابق، ص218.

اختبار الموضوع، ثم مرحلة التعبير، والابتكارية يمكن أن تظهر في مرحلة تكوُّن عناصر الموضوع وطريقة التعبير عنه، كالمختارات والتجميعات المأخوذة من مصنفات سابقة، فيمكن أن تخضع للحماية لأن الابتكار يتوافر هنا بالنظر إلى كيفية تكوين عناصر الموضوع عن طريق التجميع، وبتطبيق ذلك على برامج الحاسب الآلي نجد أنه يستجمع شروط الابتكارية باعتباره مصنفًا أدبيًا طبقًا للمعنى الوارد في اتفاقية برن الخاصة بحماية المصنفات الأدبية والفنية ووفقًا لنص المادة الأولى من التوجيه الأوروبي الخاص بالحماية القانونية لبرامج الحاسب الآلي.

وفي الحقيقة لقد اتجه البعض إلى أن إعداد برامج الحاسب الآلي يشهد بصفة كافية على توافر شخصية المؤلف، وأنه في كل مرحلة من مراحل إعداده يتضح لنا بجلاء البصمة الشخصية للمعلومات، والتي تعبر عن مجهود ذهني غير عادي من أجل إتمام جميع مراحل إعداد البرنامج[1].

وقد اتجهت بعض الآراء إلى عدم حماية برامج الحاسب الآلي بقانون حق المؤلف، وذلك لغياب البصمة الشخصية لمؤلفي البرامج، والتي تعبر عن شخصيتهم أثناء إعداد البرنامج، كما أن الطابع الجمالي غير متوافر في برامج الحاسب الآلي، ونظرًا لصعوبة البحث عن عنصر الابتكار في برامج الحاسب الآلي اتجه البعض إلى القول بضرورة البحث عن تعريف جديد للابتكارية يتناسب وبرامج الحاسب الآلي، أو بمعنى آخر يجب تحديث المعنى التقليدي للابتكارية حتى يتلاءم مع برنامج الحاسب الآلي[2].

---

(1) J. L. Coutal: La protection jumidique de logical, dalloz, 1984, Chronique, P. 199.

(2) د. شحاتة غريب محمد شلقامي، الحق الأدبي لمؤلف برامج الحاسب الآلي، دراسة في قانون حماية الملكية الفكرية الجديد رقم 82 لسنة 2002، دار الجامعة الجديدة، القاهرة، 2008، ص 76.

وقد اتجه القضاء الفرنسي إلى التأكيد على توافر البصمة الشخصية لمؤلفي برامج الحاسب الآلي في تكوينه، وفي التعبير عنه، فقد ذهبت محكمة استئناف باريس في حكم لها التأكيد على أن إعداد برامج الحاسب الآلي التطبيقية يعد عملا ذهنيًا مبتكرًا في تكوينه، وفي التعبير عنه يزيد عن كونه مجرد عمليات منطقية، فالمحللون المبرمجون يختارون ما بين العديد من طرق العرض والتعبير عن البرامج[1]، واختيارهم هذا إنما يعبر بجلاء عن شخصياتهم، فالقدرة على الاختيار هي البصمة الشخصية لمؤلفي برنامج الحاسب الآلي، وبالتالي يعتبر إعداد المبرمجين لبرامج الحاسب الآلي عملا ذهنيًا ابتكاريًا[2].

لكن اعترض بعض الفقه الفرنسي على هذا الحكم الصادر من محكمة استئناف باريس بالقول بأن برامج الحاسب الآلي لا تستوفي شرط

(1) د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص 101.

(2) ذهبت محكمة استئناف باريس إلى:

L élaborations d'un programme d'application d'ordinateur est une ouvre de l'esprit originale dans sa composition et son espressione allant au.delà d'une simple logique automatique et contraignante , qui ne s'agit pas d'un mécanisme intellectuel nécessaire, qu' en effet, les analyses programmeurs ont a choisir comme les traducteurs d'ouvrages entre divers modes de présentation et d'expression , que leur choix porte insti la marque de leur personnalité".

Ca Paris, 2 Novenre 1982, Gaz. Pal., 3 mars 1983, P. 118 , Nore J. R. Bonneau.

وقد كان أول حكم قضائي فرنسي يتبنى فكرة حماية برامج الحاسب الآلي بقانون حق المؤلف هو حكم المحكمة الابتدائية لمدينة Bobigny الصادر بتاريخ 11 ديسمبر 1979، والذي اعتبر برنامج المصدر مصنفًا أدبيًا، ويكون مبتكرًا في تكوينه أو في طريقة التعبير عنه..

الابتكارية[1].

في حين أن البعض الآخر يرى أن برنامج الحاسب الآلي يكون مصنفًا في تكوينه، وترتيبًا على ذلك يستحق برنامج الحاسب الحماية المقررة في القانون، فالبرنامج يتجاوز مجرد الفكرة، كما أن المبرمج يكون في نفس الشروط التي يكون فيها المترجم، وقانون حقوق المؤلف يحمي المترجم، فقد أشار هذا القانون للمصنفات المترجمة ضمن المصنفات المحمية بنصوصه[2].

ولتأكيد وجود البصمة الشخصية لمؤلفي برامج الحاسب الآلي نجد المحكمة الابتدائية لباريس أكدت أن المجهود الشخصي لمبتكر برنامج الحاسب الآلي يظهر في النتيجة التي نحصل عليها، كما هو الحال تمامًا بالنسبة للمؤلف الموسيقي.

ولكن هناك رأي في الفقه يعترض على الرأي القائل بأن إعداد برنامج الحاسب الآلي يشهد بالبصمة الشخصية لمؤلفه، ويستكمل هذا الرأي قوله بأن تحقيق أو إعداد البرنامج يتطلب مجهودًا ذهنيًا، ولكن لا يجب أن نخلط بين هذا المجهود وبين فكرة البصمة الشخصية، كما أن اختيار المبرمج يكون موجهًا بالتقنيات الموجودة، ويعني ذلك أن اختيار المبرمج للغة معينة يصبغ بها برنامجه لا يكون حرًا في اختيارها، بل هو مقيد بالتقنيات القائمة المحددة والتي يجب ألا يتعداها، مما يضعف فكرة وجود بصمة شخصية له عند إعداده للبرنامج.

فيرى هذا الرأي أن المصنفات الفكرية لا تستحق الحماية إلا إذا كان

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 375.

(2) J. R. Bonneau: Note sous CA de Paris, 2 Novembre 1982, Gaz. Pal. 3 mars 1983, P. 120.

الهدف منها الإعلام أو التسلية أو التثقيف، أي تحقيق متعة أدبية، لذلك فبرامج الحاسب الآلي لا تدخل في دائرة الحماية لتجردها من كل مضمون فكري وجمالي يمكن أن يكون محميًا بقانون حق المؤلف، فالحماية بهذا القانون لا تكون للمصنفات الفكرية إلا إذا خاطبت الحس الجمالي عند الإنسان، أما برامج الحاسب الآلي فهي مجرد تعليمات يقوم بها الحاسب الآلي، وليست مخاطبة للحس الجمالي عند الإنسان[1].

وقد ذهبت محكمة استئناف باريس إلى الحكم بأنه لا يمكن تشبيه إعداد برنامج الحاسب الآلي بمصنف فكري له طابع جمالي، وإذا كانت هذه البرامج تهدف إلى إعداد ألعاب، فإن ذلك مجرد تجميع تكنولوجي لا يمكننا إدراجه ضمن المصنفات الفكرية، وعلى المخترع أن يبحث في نصوص قانون الملكية الصناعية[2].

وقد اتجهت محكمة النقض الفرنسية في حكم لها عام 1986 إلى أن الحماية التشريعية تشمل كل مصنف فكري مبتكر يعبر عن شخصية مؤلفه استقلالا عن أي اعتبار للطابع الجمالي[3].

ونحن مع الرأي القائل أن برامج الحاسب الآلي يتوافر فيها قدر من الطابع الجمالي، وهي مبتكرة تعبر عن بصمات شخصية لمؤلفها، وبالتالي تخضع للحماية بقانون حق المؤلف, على أساس أن الحماية الواردة في قوانين حق المؤلف تنصب أساسًا على الانتاج الفكري مهما كانت صوره, بشرط تميزه بطابع الابتكار[4].

(1) د. محمد حسام لطفي: الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص 93 وما بعدها.
(2) CA de Pari, 4 juin 1984, RIDA, Janvier 1985, P. 178.
(3) Cass. Ass. Plénière, 7 Mars 1986, expo, no 82, P. 59 est.
(4) د. نواف كنعان, حق المؤلف, دار الثقافة للنشر, الأردن, 2000, ص 242.

كما أن الرأي القائل بأن برامج الحاسب الآلي وتنفيذها يكون مجهولا بالنسبة للغير أو للجميع ليس في محله، فقد استند هذا الرأي إلى أن برامج الحاسب الآلي عبارة عن تعبير مفهوم لمبرمجيها دون الغير أو من يستخدمها، على العكس من المصنفات الأدبية والفنية التي تكون بوضوح مفهومة للجمهور[1]، لأن تقدير الابتكارية يجب أن يخضع لقواعد خاصة بالنسبة لبرامج الحاسب الآلي، فيجب تقديرها موضوعيًا لأنها لا تتحدد بالنظر إلى المؤلف، لكنها تتحدد بالنظر إلى العمل نفسه، وقد أخذت بعض التشريعات العربية بهذه النظرة الموضوعية عند تقرير مدى توافر الابتكارية.

وفي الواقع فإن الرجوع إلى الطابع الموضوعي للابتكارية يقودنا إلى الخلط بين الابتكارية والجدة أو الحداثة، ومعنى قبول الجدة في مجال حق المؤلف أن ذلك سيؤدي إلى حدوث العديد من المشكلات في مجال حماية حق المؤلف، خاصة وأن روح قانون حق المؤلف هو حماية الابتكارية وليس الجدة أو الحداثة، لأن هذه الأخيرة مجالها في قانون براءة الاختراع، والابتكارية يجب أن تقدر بناءً على معيار شخصي وليس موضوعي، فالمصنف يكون مبتكرًا ويستفيد من الحماية بقانون حق المؤلف إذا كان معبرًا عن البصمة الشخصية لمؤلفه، والتي لا تظهر في المصنفات المنتجة بواسطة الآلة[2].

وما قيل عن برامج الحاسب الآلي ينسحب على قواعد البيانات Databasees وهي مجموعة من البيانات أو المواد الأخرى أيًا كان شكلها إذا كانت تعتبر ابتكارات فكرية بسبب اختيار محتوياتها وترتيبها.

(1) A l Lucas: Droit d'auteur et numérique: op. cit, no 67 , P. 35.

(2) A l Lucas: Droit d'auteur et numérique: op. cit, no 67 , P. 35

وقضت محكمة النقض الفرنسية في قضية Microfor – le monde بأن قيام شركة Microfor الكندية بجمع الصحف الفرنسية وتنظيمها وفهرستها وتخزينها ووضعها في متناول الجمهور يعد جهدًا فكريًا وهو بمثابة مصنف محمي بقانون حق المؤلف[1].

وفي النهاية فإن حماية مؤلفي برامج الحاسب الآلي بقانون حق المؤلف لا يشترط أن يقدموا شيئًا جديدًا، بل يكفي أن يعبر مصنفهم عن بصماتهم الشخصية، وفقًا لما أخذ به التوجيه الأوروبي الصادر في عام 1991، حول الحماية القانونية لبرامج الحاسب الآلي، وأيضًا ما أخذ به المشرع في فرنسا ومصر والإمارات.

لقد رأينا أن المشرع يحمي فكرة الإبداع والابتكار، في الأعمال الأدبية والعلمية، فهي محل تشجيع الدول، حتى إن بعضها تحميها بقواعد دستورية تقديرًا للابتكار في مجال العلوم والآداب، وتولي الدول العربية اهتمامًا كبيرًا بمسائل الملكية الفكرية، حتى إننا نجد بعضها قد ساهم في الجهد الدولي لحماية الملكية الفكرية، ونجد أن عددًا من الدول العربية كان من الدول الأساسية في إعداد العديد من اتفاقيات الملكية الفكرية الدولية، كما أننا نجد أن أغلب الدول العربية تتوفر لديها قوانين في ميدان حماية حق المؤلف والحقوق المجاورة وبراءات الاختراع والتصاميم الصناعية والعلامات التجارية.

هذا وقد شهدت نهاية التسعينيات وعام 2000 موجة تشريعية في ميدان حماية الأسرار التجارية وتعديل قوانين الملكية الفكرية تلبية لمتطلبات

---

(1) د. نواف كنعان, حق المؤلف, مرجع سابق, ص 247.
ولتفاصيل هذه القضية انظر د. محمد حسام لطفي, بنوك المعلومات وحقوق المؤلف, بدون ناشر, 1999, ص25.

العضوية في منظمة التجارة العالمية، وما يوجبه ذلك من تلبية متطلبات اتفاقية تربس التي نصت على هذه الحماية، حيث تكاد تتطابق التدابير التشريعية مع ما تتطلبه اتفاقية تربس في الموضوعات المشار إليها.



المبحث الثاني

الحماية الجنائية الدولية والوطنية

لحقوق مؤلف برامج الحاسب الآلي

يظل تحديد مفهوم المصنف الرقمي الواجب حمايته جنائيًا مثار جدل في مجال الدراسات القانونية، وربما يحتاج تحديد مفهومه وتعريفه أو توصيفه إلى حوار فقهي حوله تمهيدًا للوصول إلى رأي غالب أو إجماع، ومع ذلك فمن الضروري أن نحدد مفهوم المصنف الرقمي.

وتنتمي المصنفات المعلوماتية إلى بيئة الكمبيوتر، والتفكير في حمايتها بدأ بوصفها معدات ووسائل تقنية المعلومات، فكان نظام براءات الاختراع هو النظام المتناسب مع ذلك باعتبار براءة الاختراع ترد بشأن مخترع جديد يتصف بالابتكارية والجدة وبالقابلية للاستغلال الصناعي، وتتمثل المصنفات الرقمية في برامج الحاسوب وقواعد البيانات والدوائر المتكاملة، أما في بيئة شبكة الإنترنت فتتسمى بأسماء النطاقات أو مواقع شبكة الإنترنت.

وقد اتجهت معظم المحاولات إلى البحث في قانون حق المؤلف للتعرف على مدى ملاءمة هذا القانون لبرامج الحاسب الآلي باعتبارها مصنفات مبتكرة.

وقد بدأ الاهتمام الدولي بحماية الانتاج الفكري على المستوى الدولي في الربع الأخير من القرن الثامن عشر, بعد أن أدركت الدول التي أصدرت قوانين حق المؤلف خلال تلك الفترة أن تطبيق هذه القوانين يتطلب التعاون بينها لحماية الإنتاج الفكري, فظهرت فكرة الاتفاقيات الدولية، وكانت البداية في اتفاقية برن لحماية المصنفات الأدبية والفنية في 9 سبتمبر 1886, وهي أقدم اتفاقية دولية متعددة الأطراف لحماية حق المؤلق على المستوى

الدولي، ثم تبعتها بعد ذلك الاتفاقيات الأخرى كاتفاقية تربس، والاتفاقية الأوروبية للجريمة المعلوماتية، وهاتان الاتفاقيتان تعتبران الأحدث إذا ما قورنتا باتفاقية برن.

وتستلزم دراسة هذا المبحث عرض الجهود الدولية الرامية لتحقيق الحماية الجنائية لحقوق مؤلفي برامج الحاسب الآلي، والتي لا يمكن أن تغفل مضمون هذه الحماية وفقًا لاتفاقية التربس التي تعتبر من أهم الاتفاقيات المبرمة في إطار منظمة التجارة العالمية، وكذا اتفاقية بودابست بشأن الإجرام المعلوماتي، ثم نتبع ذلك ببيان الجهود الوطنية المتمثلة في بيان أحكام جريمة تقليد برامج الحاسب الآلي، لذلك قسمنا هذا المبحث إلى مطلبين كما يلي:

المطلب الأول: الحماية الجنائية الدولية لحقوق مؤلفي برامج الحاسب الآلي

المطلب الثاني: الحماية الجنائية الوطنية لبرامج الحاسب الآلي

المطلب الأول

الحماية الجنائية الدولية لحقوق مؤلفي برامج الحاسب الآلي

بدأ التنظيم الدولي لموضوعات الملكية الفكرية منذ نهايات القرن قبل الماضي وبالتحديد عام 1883، حيث تم توقيع (اتفاقية باريس) لحماية الملكية الصناعية، ثم اتفاقية برن لحماية المصنفات الأدبية والفنية الموقعة عام 1886، واتفاقية مدريد ولائحتها التنفيذية بخصوص التسجيل الدولي للعلامات التجارية والصناعية الموقعة عام 1891، وقد توالت بعد ذلك التشريعات الدولية المنظمة لحقوق الملكية الفكرية في مجالاتها المختلفة، حتى تكون من مجموع ذلك ما يمكن تسميته [قانون الملكية الفكرية الدولي]

وهو قانون دولي يتضمن الأحكام القانونية التي أقرها المجتمع الدولي لتنظيم موضوعات الملكية الفكرية بمقتضى معاهدات دولية[1].

وتعد من أهم الاتفاقيات الموقعة في هذا المجال اتفاقية تربس TRIPS والموقعة في 15 أبريل 1994 من 117 دولة، والخاصة بالجوانب التجارية في موضوع الملكية الفكرية.

كما تعد منظمة [الويبو WIPO] من أهم المنظمات العالمية في مجال حقوق الملكية الفكرية، وهي منظمة دولية تهدف إلى تقديم المساعدة من أجل ضمان حماية حقوق المبدعين وأصحاب الملكية الفكرية في جميع أنحاء العالم.

وتعد الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست)، من الاتفاقيات الحديثة والتي تصدت لجوانب مختلفة في المجال المعلوماتي، ومن هذه الجوانب ما يتعلق بحق المؤلف.

وسنتناول في هذا المطلب الحماية الجنائية الدولية لحقوق مؤلفي برامج الحاسب الآلي من خلال الحماية المقررة لبرامج الحاسب الآلي وفقًا لاتفاقية التربس، ونتبع ذلك بحماية برامج الحاسب الآلي في ضوء اتفاقية بودابست، كل في فرع على حدة على النحو التالي:

الفرع الأول

الحماية الجنائية لبرامج الحاسب الآلي وفقًا لاتفاقية التربس

تحمى حقوق الملكية الفكرية بواسطة التشريع الوطني، في حين أن الحماية الدولية ترسم حدودها المعاهدات والاتفاقيات الدولية، ولعل أهم حدث قانوني تجلى في توقيع معظم دول العالم على اتفاقية الجات الجديدة

(1) فاروق علي الحفناوي، قانون البرمجيات، مرجع سابق، ص 72.

وقيام منظمة التجارة العالمية، ونظرًا لأهمية الملكية الفكرية بالنسبة للأمور التجارية، فقد بذلت جهود كثيرة لإرساء نظم للملكية الفكرية أكثر فاعلية وتجانسًا، ومن أهم تلك الجهود التوقيع على اتفاقية جوانب التجارة المتصلة بحقوق الملكية الفكرية 1994[1] كجزء من جولة أورجواي للمفاوضات التجارية متعددة الأطراف، والتي أنشأت منظمة التجارة العالمية.

وهذه الاتفاقية التي يشار إليها باتفاقية التربس لا تتضمن فقط معايير للحماية يجب أن يتبناها أعضاء المنظمة، ولكنها أيضًا تضع الإجراءات التي يجب أن تتبناها الدول الأعضاء لتطبيق حقوق الملكية الفكرية، كما أنها أيضًا تتضمن بعض الالتزامات المتعلقة بإدارة نظم الملكية الفكرية، والملاحظ أن هذه الاتفاقية أعطت لموضوع الملكية الفكرية بشكل عام بعدًا عالميًا، وربطت موضوعات الملكية الفكرية بآليات دولية محددة قد لا تستطيع دول كثيرة الفكاك منها، ومن الموضوعات التي تناولتها الاتفاقية تناولا صريحًا موضوع الحماية الجنائية لبرامج الكمبيوتر[2].

وتعد معايير هذه الاتفاقية معايير مكملة وليست معايير بديلة لتلك المعايير التي وردت في معاهدات الملكية الفكرية الأخرى، فمثلا معظم الالتزامات الجوهرية التي نصت عليها اتفاقية برن بشأن الحماية الجنائية للمصنفات الأدبية والفنية تضمنتها بالإشارة اتفاقية التربس من خلال مادتها التاسعة، فتطبق على جميع أعضاء منظمة التجارة العالمية حتى ولو لم ينضموا إليها، وبالمثل فإن الالتزامات الجوهرية لاتفاقية باريس قد تضمنتها اتفاقية التربس من خلال المادة الثانية.

---

(1) تعتبر هذه الاتفاقية من أهم الاتفاقيات الدولية في القرن العشرين، والدول التي وقعت عليها هي الدول الأعضاء في منظمة التجارة.

(2) فاروق علي الحفناوي , قانون البرمجيات, مرجع سابق, ص 113.

وتفرض معظم أحكام اتفاقية التربس التزامات بضرورة تشجيع الحماية الفعالة أكثر مما تطلبته الاتفاقيات الدولية السابقة الخاصة بالملكية الفكرية، وفي حالات نادرة نجد أن معايير اتفاقية التربس تتداخل مع الاتفاقيات الدولية للملكية الفكرية مما يفرض التزامات مزدوجة، ومن أمثلة ذلك متطلبات المعاملة الوطنية، والدولة الأولى بالرعاية الموجودة باتفاقية التربس، ويمكن لجميع أعضاء اتفاقية التربس الاستفادة منها.

كما أن بعض الاتفاقيات الأخرى مثل اتفاقية التجارة الحرة لشمال أمريكا تفرض على أعضائها معايير أفضل من التي تفرضها اتفاقية التربس.

وتتنوع الوسائل الكفيلة بحماية برامج الحاسب الآلي في إطار اتفاقية التربس، والتي من بينها ما تنص عليه المادة العاشرة منها في فقرتها الأولى أن تتمتع برامج الحاسب الآلي والكمبيوتر سواء أكانت بلغة المصدر أو بلغة الآلة[1] بالحماية الجنائية باعتبارها أعمالا أدبية بموجب معاهدة برن 1971.

أما الفقرة الثانية من المادة 10 فقد نصت على أن: " تتمتع بالحماية البيانات المجمعة أو المواد الأخرى، سواء أكانت في شكل مقروء آليًا أو أي شكل آخر، إذا كانت تشكل خلقًا فكريًا نتيجة انتقاء أو ترتيب محتوياتها، وهذه الحماية لا تشمل البيانات أو المواد في حد ذاتها، ولا تخل بحقوق

---

(1) برامج الحاسب الآلي تكتب بلغة عالية المستوى تسمى لغة المصدر، ولكي يعمل هذا البرنامج على الحاسب لابد من ترجمته إلى اللغة الوحيدة التي تفهمها المكونات المادية للحاسب وهي لغة الآلة، ولهذا يطلق على البرنامج بعد تحويله إليها برنامج الهدف، وقد جرى العمل في عقود البيع الواردة على برامج سابقة الإعداد أن يطرح للبيع برنامج الهدف فقط، أما برنامج المصدر فيحتفظ به المنتج. انظر في هذا الصدد: د. أسامة محمد محيي الدين، مدخل الحاسب الآلي ونظم المعلومات، مرجع سابق، ص 127.

المؤلف المتعلقة بهذه البيانات أو المواد ذاتها". ويبدو أن هـذه الفقـرة قـررت حمايـة للبيانـات المجمعة أو المواد الأخرى وذلك بشروط معينة.

وجدير بالذكر أن هناك حماية عامة لبرامج الكمبيوتر فرضتها اتفاقية أوجه التجارة المتصلة بحقوق الملكية الفكرية (التربس)، فمن ناحيـة أولى هنـاك التـزام عـلى عـاتق الـدول الأعضـاء في الاتفاقية بضمان أن تشتمل قوانينهـا مجموعـة مـن الإجـراءات لإنفـاذ حقـوق الملكيـة الفكريـة المنصوص عليها في هذا الجزء من الاتفاقية، وذلك بهدف تسهيل اتخاذ تدابير فعالة ضـد أي تعـدٍّ على حقوق الملكية الفكرية التي تغطيها الاتفاقية، وكـذلك اتخـاذ إجـراءات سريعـة لمنـع بعـض التعديات وردع التعديات الأخرى[1]، ثم

---

(1) نص المادة 41 من اتفاقية التربس:

(1) تلتزم البلدان الأعضاء بضمان اشتمال قوانينها لإجـراءات الإنفـاذ المنصـوص عليهـا في هـذا الجـزء لتسـهيل اتخاذ تدابير فعالة ضد أي تعدٍّ على حقـوق الملكيـة الفكريـة التـي تغطيهـا هـذه الاتفاقيـة، بمـا في ذلـك الجزاءات السريعة لمنـع التعـديات، والجـزاءات التـي تشـكل رادعًـا لأي تعـديات أخـرى، وتطبـق هـذه الإجراءات بالأسلوب الذي يضمن تجنب إقامة حواجز أمام التجارة المشروعة ويوفر ضمانات ضد إسـاءة استعمالها.

(1) تكون إجـراءات إنفـاذ حقـوق الملكيـة الفكريـة منصـفة وعادلـة، ولا يجـوز أن تكـون معقـدة أو باهظـة التكاليف بصورة غير ضرورية، ولا أن تنطوي على حدود زمنية غير معقولة أو تأخير لا داعي له.

(1) يفضل أن تكون القرارات المتخذة بصدد موضوع أي من القضايا مكتوبة ومعللة، وتتم إتاحتهـا عـلى الأقـل للأطراف المعنية بالقضية دون أي تأخير لا لزوم له، وألا تستند تلك القرارات إلا إلى الأدلة التـي أعطيـت للأطراف المعنية فرصة عرض وجهة نظرها فيها.

(1) تتاح للأطراف محل دعوى في قضية ما فرصة لأن تعرض على سلطة قضائية القرارات الإدارية النهائية، ومـع مراعاة الاختصاصات التي تنص عليها قوانين البلد العضو فـيما تتصـل بأهميـة تلـك القضـية، عـلى الأقـل الجوانب القانونية للأحكام =

ضرورة توافر مجموعة إجراءات قضائية مدنية إلى جانب إجراءات إدارية أخرى[1]، وفي هذا الإطار العام تلتزم البلدان الأعضاء في الاتفاقية بمراعاة أحكام المواد من 1 إلى 21 من معاهدة برن عام 1971 وملحقاتها، مع مراعاة أن هذه الحماية تسري فقط على النتاج وليس مجرد الأفكار أو الإجراءات أو أساليب العمل أو المفاهيم الرياضية[2]، وأخيراً تتمثل الحماية

= القضائية الأولى المتخذة بصدد موضوع هذه القضية، غير أنه لا تلزم البلدان الأعضاء بإتاحة فرصة لإعادة النظر في القضايا الجنائية التي صدرت أحكام ببراءة المتهمين فيها.

(1) من المفهوم أن هذا الجزء لا ينشئ أي التزام بإقامة نظام قضائي خاص بإنفاذ حقوق الملكية الفكرية منفصل عن النظام الخاص بإنفاذ القوانين بصفة عامة، ولا يؤثر على قدرة البلدان الأعضاء على إنفاذ قوانينها بصفة عامة، ولا ينشئ أي من الأحكام التي ينص عليها هذا الجزء التزامًا فيما يتصل بتوزيع الموارد بين إنفاذ حقوق الملكية الفكرية وإنفاذ القوانين بصفة عامة.

(1) المادة 42 الإجراءات المنصفة والعادلة:

تتيح البلدان الأعضاء لأصحاب الحقول (11) إجراءات قضائية مدنية فيما يتصل بإنفاذ أي من حقوق الملكية الفكرية التي تغطيها هذه الاتفاقية، وللمدعى عليهم الحق في تلقي إخطار مكتوب في الوقت المناسب يحتوي على قدر كاف من التفاصيل، بما في ذلك الأساس الذي تستند إليه المطالبات، ويسمح للأطراف المتخاصمة بأن يمثلها محامون مستقلون، ولا يجوز أن تفرض الإجراءات متطلبات مرهقة أكثر مما ينبغي فيما يتعلق بالإلزام بالحضور شخصيًا، وتعطى كافة الأطراف المتخاصمة الحق في إثبات مطالباتها وتقديم كافة الأدلة المتصلة بالقضية، وتصبح الإجراءات وسائل تحديد المعلومات السرية وحمايتها ما لم يكن ذلك مخالفًا لنصوص الدساتير القائمة.

(2) المادة 9 العلاقة مع معاهدة برن:

1) تلتزم البلدان الأعضاء بمراعاة الأحكام التي تنص عليها المواد من 1 وحتى 21 من معاهدة برن (1971م) وملحقها، غير أن البلدان الأعضاء لن تتمتع بحقوق ولن تتحمل التزامات بموجب هذه الاتفاقية فيما يتعلق بالحقوق المنصوص=

الزمنية لهذه المصنفات خلال حياة المؤلف بالإضافة إلى مدة خمسين عامًا بعد وفاته[1].

الفرع الثاني

حماية برامج الحاسب الآلي في ضوء اتفاقية بودابست

نصت اتفاقية بودابست الخاصة بالإجرام الافتراضي أو الكوني لسنة 2001 على الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة من خلال المادة العاشرة[2] والتي تنص على أنه:

= عليها في المادة 6 مكرر من معاهدة برن أو الحقوق النابعة عنها.

2) تسري حماية حقوق المؤلف على النتائج وليس على مجرد الأفكار أو الإجراءات أو أساليب العمل أو المفاهيم الرياضية.

(1) المادة 12 مدة الحماية:

عند حساب مدة حماية عمل من الأعمال - خلاف الأعمال الفوتوغرافية أو الأعمال الفنية التطبيقية - على أساس آخر غير مدة حياة الشخص الطبيعي، لا تقل هذه المدة عن 50 سنة اعتبارًا من نهاية السنة التقويمية التي أجيز فيها نشر تلك الأعمال، أو في حال عدم وجود ترخيص بالنشر في غضون 50 سنة اعتبارًا من إنتاج العمل المعني، تكون مدة الحماية 50 سنة اعتبارًا من نهاية السنة التقويمية التي تم فيها إنتاجه.

(2) **Article 10، Offences related to infringements of copyright and related rights**

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade،Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed

1) تقوم كل دولة طرف بالاتفاقية بإقرار هذه الإجراءات التشريعية وغيرها من الإجراءات الأخرى، كلما كان ذلك ضروريًا لإصدار نص تشريعي أو قانوني بأنها تشكل جرائم بموجب القانون الوطني المحلي الخاص بها، وذلك من حيث مخالفة أو انتهاك حقوق الطبع والنشر كما هو محدد وفقًا للقانون الخاص بهذه الدولة الطرف بالاتفاقية وفقًا للالتزامات التي تم التوقيع عليها في ظل الاتفاقية لحق المؤلف الموقعة في باريس في 24 يوليو 1971، واتفاقية برن لحماية الأعمال الأدبية والفنية، واتفاقية الجوانب التجارية لحقوق الملكية الفكرية، واتفاقية المنظمة العالمية للملكية الفكرية (WIPO) - باستثناء أي حق معنوي ممنوح بواسطة هذه الاتفاقيات - إذا ما

---

wilfully, on a commercial scale and by means of a computer system.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade‚Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5‚ Ancillary liability and sanctions

ارتكبت هذه الأفعال عمدًا، وعلى نطاق تجاري، وبواسطة نظام معلوماتي.

2) يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية من أجل تجريم - تبعًا لقانونه الداخلي - انتهاكات الحقوق المجاورة المعرفة في قانون هذا الطرف، وفقًا للالتزامات التي تم التوقيع عليها في ظل الاتفاقية الدولية المبرمة في روما لحماية الفنانين، والمؤدين أو العازفين، أو منتجي الصوتيات ومنظمات البث - اتفاقية روما للجوانب التجارية لحقوق الملكية الفكرية، كذلك اتفاقية المنظمة الدولية للملكية الفكرية- باستثناء أي حق معنوي منصوص عليه بواسطة هذه الاتفاقيات، إذا ارتكبت هذه الأفعال عمدًا وعلى نطاق تجاري، أو بواسطة نظام معلوماتي.

3) يمكن لأي طرف - في ظل ظروف محدودة للغاية - أن يحتفظ بالحق في عدم تطبيق المسئولية الجنائية، بالنسبة للفقرتين الأولى والثانية من هذه المادة، بشرط توافر طرق أخرى فعالة وجاهزة، وألا يكون في هذا التحفظ ما يحمل اعتداءً على الالتزامات الدولية المفروضة على هذا الطرف، في تطبيق الاتفاقيات الدولية المشار إليها في الفقرتين الأولى والثانية من هذه المادة.

وتؤكد المذكرة التفسيرية[1] على أن انتهاكات حقوق الملكية الفكرية - وعلى الأخص حق المؤلف - تعتبر من بين الجرائم الأكثر انتشارًا على شبكة الإنترنت، وتشير المذكرة إلى أن إعادة إنتاج وبث الأعمال المحمية عبر شبكة الإنترنت دون موافقة حائز حق المؤلف هو من الأمور التي

(1) Convention sur la cybercriminalité. STE. no. 185, Rapport explicatif adopte le 8 novembre 2001, P. 27 etS.

انتشرت، وهذه الأعمال المحمية تشتمل على وجه الخصوص الأعمال الأدبية والتصويرية والموسيقية، والسمعية البصرية، ثم إنه من السهل إجراء نسخ غير مصرح به عن طريق التكنولوجيا الرقمية، وبالتالي إعادة الإنتاج والتوزيع عبر الشبكات الإلكترونية، مما يستلزم وضع نصوص تتضمن جزاءات جنائية وتعزز التعاون الدولي في هذا الإطار.

وتلزم المادة العاشرة من المذكرة التفسيرية كل طرف بتحريم الانتهاكات العمدية على الملكية الفكرية، وعلى الحقوق المتصلة[1]، إذا كانت هذه الانتهاكات قد تم ارتكابها عن طريق نظام معلوماتي وعلى نطاق تجاري[2].

وتقرر المادة المذكورة في الفقرة الأولى جزاءات جنائية ضد انتهاكات الملكية الفكرية المرتكبة باستخدام نظام معلوماتي، أما الفقرة الثانية من هذه المادة فإنها تركز على انتهاكات الحقوق المجاورة التي يتم ارتكابها باستخدام نظام معلوماتي.

والملاحظ أن الالتزام بالتجريم الوارد في الاتفاقية لا يغطي انتهاكات الملكية الفكرية غير تلك المنصوص عليها صراحة في المادة العاشرة، وبالتالي يتم استبعاد انتهاكات براءات الاختراع والعلامات التجارية وباقي حقوق الملكية الصناعية[3].

وتحيل الفقرة الأولى إلى اتفاقية باريس لحماية الملكية الصناعية، واتفاقية برن لحماية الأعمال الأدبية والفنية، واتفاقية الجوانب التجارية

(1) يشار إليها تحت عنوان الحقوق المجاورة.

(2) د. هلالي أحمد عبداللاه، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، دار النهضة العربية، 2003، ص 135.

(3) د. هلالي عبد اللاه أحمد، اتفاقية بودابست لمكافحة جرائم المعلوماتية، مرجع سابق، ص 136.

لحقوق الملكية الفكرية، ومعاهدة حقوق المؤلف للمنظمة الدولية للملكية الفكرية.

أما الفقرة الثانية، فإنها تحيل إلى اتفاقية روما الدولية لحماية المؤدين والعازفين ومنتجي الصوتيات ومنظمات البث، واتفاقية الجوانب التجارية لحقوق الملكية الفكرية، واتفاقية المنظمة الدولية الفكرية بالنسبة لأعمال الأداء والعزف والبث.

وتتجه نصوص اتفاقية بودابست إلى فرض جزاءات جنائية ضد الانتهاكات المرتكبة على نطاق تجاري وعن طريق نظام معلوماتي، وهذا يتفق مع المادة (61) من اتفاقية الجوانب التجارية لحقوق الملكية الفكرية، والتي لا تفرض عقوبات جنائية في حالة المس بحق المؤلف إلا في حالة القرصنة على نطاق تجاري، لكن استثناءً يمكن للأطراف أن يتجاوزوا النطاق التجاري، وذلك بتجريم صور أخرى لانتهاك حقوق الملكية الفكرية[1].

ويتمثل الركن المعنوي للجرائم المرتبطة بحق المؤلف والحقوق اللصيقة في القصد الجنائي العام بعنصريه العلم والإرادة، فهي جريمة عمدية، فقد اشترطت المادة (10) أن يكون هناك عمد لتحقق الجريمة وتقرير المسئولية الجنائية، وهذا ما ذهبت إليه كذلك المادة (61) المتعلقة بالالتزام بتجريم انتهاكات حق المؤلف في اتفاقية الجوانب التجارية لحقوق الملكية الفكرية.

أما الفقرة الثالثة من المادة العاشرة فإنها سمحت للأطراف استثناءً بعدم تطبيق المسئولية الجنائية في الفقرتين الأولى والثانية في ظروف محددة للغاية.

(1) المرجع السابق، ص 140.

المطلب الثاني

الحماية الجنائية الوطنية لبرامج الحاسب الآلي

أقرت الأحكام القضائية العديدة ضرورة حماية برامج الحاسب الآلي بقانون حق المؤلف، كما جاءت تشريعات غالبية الدول مقننة لهذا الوضع العام، وأدرجت برامج الحاسب الآلي ضمن المصنفات الفكرية الخاضعة لنصوص قانون حق المؤلف، فلم يعد الأمر كما كان من قبل متعلقًا بالبحث عن مدى اعتبار برنامج الحاسب الآلي مصنفًا مبتكرًا أم لا، فقد تم حسم الأمر من خلال مواقف المشرع الصريحة بالنص على حماية برامج الحاسب الآلي بقانون حق المؤلف.

وتعد الملكية الفكرية حجر الزاوية وأساس الإبداع في أي مجتمع من المجتمعات؛ لأنها تؤدي إلى تقدم هذا المجتمع وازدهاره، ومن أجل ذلك حرصت الدول على سن التشريعات المناسبة لحمايتها من أي اعتداء قد يقع عليها، وأصبحت إحدى أهم الصادرات التي تعتمد عليها الدول.

وتعتبر حقوق المؤلف إحدى مجموعات الحقوق التي تنبثق عن الملكية الفكرية، وأهم هذه الحقوق التي يعد الاعتداء عليها ليس اعتداءً على حقوق الأفراد المادية والمعنوية ولا مساسًا بحرية البحث العلمي والإبداع فقط، وإنما اعتداء على المجتمع بأسره.

والحماية التشريعية لحقوق المؤلف ليست بجديدة، وإنما نصت عليها بعض الدساتير قبل النص عليها في القوانين، فدستور الولايات المتحدة الأمريكية في المادة (أ) من القسم (8) نص على أنه: (يكون للكونجرس سلطة... دعم تقديم العلم والفنون النافعة، بكفالة الحقوق المطلقة لمدد محددة للمؤلفين والمخترعين على كتاباتهم واختراعاتهم).

وأكمل تشريع شامل في هذا المجال هو قانون حق المؤلف الصادر عـام 1976، والتعـديلات التـي أدخلت عليه في عام 1980 جعلته أكثر تمشيًا مع التقدم التكنولوجي[1]، وقد تم النص فيه صراحة على حماية حقوق المؤلف على برامج الحاسب الآلي.

وفي عام 1997 وبعد مطالبة ملحة من جانب القضاء الأمريكي, أصدر المشرع الأمريكي قانون النسخ عبر الإنترنت[2].

وفي فرنسا يرجع تاريخ حماية حق المؤلف إلى المرسوم بقانون الصادر في 13 يناير 1791، ثـم في 19 يوليو 1793، والمادة (428) من قانون العقوبات الفرنسي فيما يتعلق بـالمؤلفين المسرحيين، وظل القضاء الفرنسي في حمايته لسائر حقوق المؤلفين استنادًا إلى المرسومين سالفي الـذكر، حتـى تدخل المشرع الفرنسي وقنن أحكام القضاء بتشريع 11 مارس 1975، وظل القضـاء مـترددًا حـول مد الحماية للبرامج المعلوماتية، حتى صدور قانون 3 يوليو 1985 والخـاص بالكيانـات المنطقيـة، والذي أخضع البرامج المعلوماتية لحماية حق المؤلف.

(1) برنارد أ. جالر، الملكية الفكرية وبرامج الحاسبات، الجمعية المصرية لنشر المعرفة والثقافـة العالميـة، 1998، ص 15.

(2) عرف هذا القانون بقانون السرقة الإلكترونية The no Electronic Theft Act (NET) ومن أولى القضـايا التي نظرها القضاء الأمريكي وفقا لهذا القانون قضية Christian Morley حيث أدين بالاشـتراك مـع 16 شخصًا من داخل الولايات المتحدة الأمريكية ومن خارجها بتهمـة نسـخ مـا يقـارب خمسـة آلاف برنـامج كانت مخبأة في مواقع عبر شبكة الإنترنت تابعة لإحدى الجامعات في كيبيك بكندا.
انظر حول ذلك:

www.cybercrime.gov/pwaverdict.htm

د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, مرجع سابق, ص316.

وفي دولة الإمارات العربية المتحدة وحتى عام 1992 لم يكن هناك أية قوانين للملكية الفكرية، وفي سنة 1992 أصدرت الدولة ثلاثة قوانين وهي:

1) القانون الاتحادي رقم (37) لسنة 1992 في شأن العلامات التجارية، والذي يشمل حماية العلامات التجارية وعلامات الخدمة، وقد حدد الجهة المسئولة عن تسجيل هذه العلامات وهي وزارة الاقتصاد والتجارة.

2) القانون الاتحادي رقم (40) لسنة 1992 في شأن حماية المصنفات الفكرية وحقوق المؤلف.

3) القانون الاتحادي رقم (44) لسنة 1992 في شأن تنظيم وحماية الملكية الفكرية الصناعية لبراءات الاختراع والرسوم والنماذج الصناعية.

وحيث كان ذلك ونتيجة للتطور الذي شهدته المصنفات الفكرية في شتى المجالات، وتمشيًا مع الالتزامات الدولية، أصدرت دولة الإمارات العربية المتحدة القانون الاتحادي رقم (7) لسنة 2002 بشأن حقوق المؤلف والحقوق المجاورة، والذي حل محل القانون الاتحادي رقم (40) لسنة 1992، والذي كان معمولا به سابقًا.

وفي جمهورية مصر العربية كان هناك قانون حق المؤلف المصري رقم 354 لسنة 1954، والمعدل بالقانون 38 لسنة 1992 وحل محله ومحل سائر قوانين الملكية الفكرية في مصر قانون حماية الملكية الفكرية رقم 82 لعام 2002 والذي نص في مادته الثانية على إلغاء القوانين السابقة، وإلغاء كل حكم يخالف أحكامه.

وتعد جريمة تقليد المصنفات من أهم الجرائم التي تنتهك باستخدام تقنية المعلومات، والتي تكاد تكون متصلة بموضوع التجارة الإلكترونية وقد

تناولتها معظم قوانين حق المؤلف، وسوف نتناول الجرائم الماسة ببرامج الحاسب الآلي, مع التركيز على جريمة التقليد وبيان أركانها (الفرع الأول)، ثم بيان الجرائم الواردة في قانون حقوق المؤلف والحقوق المجاورة الإماراتي (الفرع الثاني).

الفرع الأول

الجرائم الماسة ببرامج الحاسب الآلي

تنص المادة الثالثة والأربعون من القانون العربي النموذجي لحماية الملكية الفكرية على أنه:

1) مع عدم الإخلال بأية عقوبة أشد واردة في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس الذي لا يقل عن (...) ولا يزيد على (...) والغرامة التي لا تقل عن (...) ولا تزيد على (...) أو بإحدى هاتين العقوبتين، كل من اعتدى على حق من الحقوق الأدبية أو المالية للمؤلف أو لأصحاب الحقوق المجاورة وفقًا لأحكام هذا التشريع، ويعد اعتداءً بوجه خاص قيام المعتدي بفعل أو بأكثر مما يلي:

أ) البيع أو الطرح للتداول، بأية صورة من الصور لمصنف محمي طبقًا لأحكام هذا التشريع.

ب) التقليد في الداخل لمصنف منشور في الخارج أو طرحه للتداول أو تصديره أو شحنه إلى الخارج مع العلم بتقليده.

ج) الإتاحة للجمهور أو أداء بث إذاعي أو تسجيل سمعي أو وضعه في متناوله عبر شبكة اتصالات تعمل بواسطة الحاسبات ما دام ذلك يتم لغرض تجاري.

د) الإزالة أو المسخ بدون وجه حق لأية حماية تقنية تنظم أو تقيد اطلاع

الجمهور على المصنف أو الأداء أو البث أو التسجيل، أو التوزيع أو الاستيراد بغرض التوزيع أو البث أو الإتاحة للجمهور، لشيء مما تقدم، ويشترط في ذلك أن يكون مرتكب الفعل عالمًا أو في إمكانه أن يعلم بالاعتداء الواقع.

2) تتعدد العقوبات بتعدد المصنفات أو الأداء أو البث أو التسجيل محل الجريمة.

3) في حالة العود تكون العقوبة أشد (مثل الحبس والغرامة على أن يضاعف مرة واحدة الحدان الأدنى والأقصى للعقوبات المنصوص عليها في الفقرة الأولى من هذه المادة).

4) في جميع الأحوال السالفة الذكر تلتزم المحكمة بأن تقضي بما يلي:

أ) مصادرة النسخ المخالفة أو المتحصلة من المخالفة.

ب) مصادرة المعدات والأدوات المستخدمة في ارتكاب أي من الأفعال المادية الواردة أعلاه.

ج) نشر ملخص الحكم الصادر بالإدانة في جريدة يومية أو أكثر على نفقة المحكوم عليه.

يجوز للمحكمة الحكم بمصادرة النسخ المخالفة أو المتحصلة من المخالفة حتى في حالة الحكم بالبراءة، كما يجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة التي استغلها المعتدون أو شركاؤهم في ارتكاب أحد الأفعال السابقة مدة لا تزيد على ستة أشهر.

كما نص القانون المصري بشأن حماية حقوق الملكية الفكرية رقم (82) لسنة 2002 في المادة (181) منه على الجرائم المتصور وقوعها على حق المؤلف بالقول بأنه: (مع عدم الإخلال بأية عقوبة أشد في قانون آخر، يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسة آلاف جنيه

ولا تجاوز عشرة آلاف جنيه، أو بأحد هاتين العقوبتين كل من ارتكب أحد الأفعال الآتية:

أولا: بيع أو تأجير مصنف أو تسجيل صوتي أو برنامج إذاعي محمي طبقًا لأحكام هذا القانون، أو طرحه للتداول بأية صورة من الصور بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.

ثانيًا: تقليد مصنف أو تسجيل صوتي أو برنامج إذاعي، أو بيعه أو عرضه للبيع أو للتداول أو للإيجار مع العلم بتقليده.

ثالثًا: التقليد في الداخل لمصنف أو تسجيل صوتي أو برنامج إذاعي منشور في الخارج، أو بيعه أو عرضه للبيع أو التداول أو للإيجار أو تصديره إلى الخارج مع العلم بتقليده.

رابعًا: نشر مصنف أو تسجيل صوتي أو برنامج إذاعي أو أداء محمي طبقًا لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكة المعلومات أو شبكات الاتصالات أو غيرها من الوسائل بدون إذن كتابي مسبق من المؤلف أو صاحب الحق المجاور.

خامسًا: التصنيع أو التجميع أو الاسترداد بغرض البيع أو التأجير لأي جهاز أو وسيلة أو أداة مصممة أو معدة للتحايل على حماية المؤلف أو صاحب الحق المجاور، كالتشفير أو غيره.

سادسًا: الإزالة أو التعطيل أو التعييب بسوء نية لأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره.

سابعًا: الاعتداء على أي حق أدبي أو مالي من حقوق المؤلف أو من الحقوق المجاورة المنصوص عليها في هذا القانون.

وتتعدد العقوبة بتعدد المصنفات أو التسجيلات الصوتية أو البرامج الإذاعية أو الأداءات محل الجريمة، وفي حالة العود تكون العقوبة الحبس

مدة لا تقل عن ثلاثة أشهر، والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه، وفي جميع الأحوال تقضي المحكمة بمصادرة النسخ محل الجريمة أو المتحصلة منها، وكذلك المعدات والأدوات المستخدمة في ارتكابها، ويجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة التي استغلها المحكوم عليه في ارتكاب الجريمة مدة لا تزيد عن ستة أشهر، ويكون الغلق وجوبيًا في حالة العود في الجرائم المنصوص عليها في البندين (ثانيًا، ثالثًا) من هذه المادة، وتقضي المحكمة بنشر ملخص الحكم الصادر بالإدانة في جريدة يومية أو أكثر على نفقة المحكوم عليه).

وعرف المشرع المصري النسخ في المادة (138) من القانون سالف الذكر بأنه استحداث صورة أو أكثر مطابقة للأصل من مصنف أو تسجيل صوتي بأية طريقة أو في أي شكل بما في ذلك التخزين الإلكتروني الدائم أو الوقتي للمصنف أو التسجيل الصوتي).

وتبقى جريمة تقليد برامج الحاسب الآلي من أهم صور الاعتداء على حقوق مؤلفيها، وقد كانت أول جريمة قرصنة وقعت في العالم في فنلندا عام 1968، حيث نسب للمتهم قيامه بالقرصنة عن طريق تقليده لبرامج الحاسب الآلي[1].

والتقليد يعني محاكاة برنامج بصنع أو إنتاج نسخ على مثاله، بحيث تبدو عند تسويقها كالأصل.

وعرفت الجريمة بأنها كل اعتداء مباشر أو غير مباشر على حقوق التأليف في مصنفات الغير واجبة الحماية[2].

(1) Daniel Padoin,la criminalite informatique le role de la police judiciaire gaz pal 1996,Dossier special p.1306.

(2) د. نواف كنعان, حق المؤلف, مرجع سابق, ص 485.

وسوف نتعرض للركن المادي والركن المعنوي لهذه الجريمة

أولا: الركن المادي لجريمة تقليد برامج الحاسب الآلي:

يتكون الركن المادي من سلوك إجرامي ونتيجة إجرامية وعلاقة سببية بينهما، ويتمثل النشاط الإجرامي في جريمة التقليد في قيام الجاني بأحد أفعال التقليد المنصوص عليها قانونًا، وتتحقق النتيجة الإجرامية بمجرد ارتكاب الفعل المؤثم، ولابد من توافر علاقة السببية بين النشاط الإجرامي وتلك النتيجة، وواضح هنا أن النشاط الإجرامي يجتمع فيه السلوك والنتيجة وعلاقة السببية بينهما، لتعاصر السلوك والنتيجة واندماج العنصرين في علاقة السببية، وسوف نعالج الركن المادي لجريمة التقليد على النحو التالي:

1- محل النشاط الإجرامي:

المصنف المحمي هو محل النشاط الإجرامي في جريمة التقليد[1]، ولن نتعرض بالتفصيل لكل أنواع المصنفات المحمية التي نصت عليها قوانين حماية حقوق الملكية الفكرية، وإنما نقتصر فقط على حماية برامج الحاسب الآلي.

وقد نص المشرع المصري على حماية هذه البرامج وقواعد البيانات من خلال قانون حماية الملكية الفكرية[2].

(1) د. علي عبد القادر القهوجي: الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، بحيث مدم لمؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، دبي الإمارات العربية المتحدة / 26 - 28 أبريل 2003، ص 98.

(2) حيث كانت هذه الحماية مثار جدل كبير في فرنسا قبل تدخل المشرع الفرنسي بالنص عليها صراحة في القانون رقم 85/ 660 الصادر في 3 يوليه 1985، وكان الفقه والقضاء هناك منقسمين حول امتداد حماية حق المؤلف إلى برامج الحاسب الآلي بسبب الاختلاف حول توافر شروط المصنف المحمي في هذه البرامج.

كما أن المشرع الإماراتي قرر الحماية لهذه البرامج وفي استحقاق هذه الحماية من عدمه فالعبرة بتوافر شروط المصنف المحمي في برامج الحاسب الآلي أو قواعد البيانات أو عدم توافرها وبصفة خاصة شرط الابتكار[1]، وهو ما يدخل في اختصاص محكمة الموضوع، ذلك أن البرنامج لا يستفيد من هذه الحماية إلا إذا كان يعكس شخصية من ينسب إليه، فالطابع الشخصي لمعد البرنامج أو بصمته الشخصية يجب أن يكون بارزًا حتى تتمتع هذه البرامج بالحماية، فالابتكار يعني أن المصنف يتميز بطابع أصيل، أي أن يكون المؤلف قد أضاف من عبقريته إلى فكرة سابقة ما يجعل لها طابعًا جديدًا يسمح بتمييز المصنف عما كان عليه من قبل[2].

وتنسحب حماية برامج الحاسب الآلي على كل مراحل إعداد البرامج، وليس على مرحلة بعينها متى توافر شرط الابتكار بإحداها[3]، وتستفيد من حماية حق المؤلف كل أنواع البرامج، وأيًا كانت الدعامة المثبت عليها

(1) د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص87.

(2) د. عبد المنعم فرج الصدة، محاضرات في القانون المدني، حق المؤلف في القانون المصري، مطبوعات جامعة الدول العربية، معهد البحوث والدراسات العربية، القاهرة، 1967، ص 15، د. حسن كيرة، المدخل إلى القانون، دار النهضة العربية، بيروت، 1967، ص 609 وما بعدها، د. توفيق حسن فرج، المدخل للعلوم القانونية، مكتبة مكاوي، بيروت، 1975، ص 554 وما بعدها، د. مصطفى الجمال، والدكتور عبد الحميد الجمال، مبادئ القانون، الكتاب الثاني، العلاقات القانونية، الفتح للطباعة والنشر الإسكندرية، 1992، ص 183، د. محمد حسام لطفي، النظام القانوني لحماية الحقوق الذهنية في مصر، بحث منشور في كتاب ندوة حقوق المؤلف الفكرية في مصر والمشار إليه سابقًا، ص 706، د. عبد السميع عبد الوهاب أبو الخير، الحق المالي للمؤلف في الفقه الإسلامي والقانوني المقارن، مكتبة وهبة، القاهرة، 1988، ص 34.

(3) د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص92 وما بعدها.

البرنامج ورق أو شريط ممغنط أو خلافه، وسواء أكان الأمر يتعلق بالنسخة الأصلية من البرنامج أم بنسخته الاحتياطية، وتمتد الحماية كذلك إلى قواعد البيانات أو ما يماثلها، سواء أكانت مقروءة من الحاسب الآلي أو من غيره، على أن يتوافر شرط الابتكار في هذه المصنفات، وذلك متروك لتقدير محكمة الموضوع[1].

2- النشاط الإجرامي:

يتمثل النشاط الإجرامي في الاعتداء على حق من حقوق المؤلف، ويتحقق ذلك بوقوع الاعتداء بالفعل، كما يجب أن يكون هذا الاعتداء قد وقع بدون إذن المؤلف، أي أن النشاط الإجرامي في جريمة التقليد له وجهان: إيجابي وهو الاعتداء، وسلبي وهو عدم الحصول على موافقة المؤلف، ويكفي الاعتداء على حق واحد من هذه الحقوق لقيام الجريمة، كما يجرم المشرع الاعتداء بكافة صوره وأيًا كانت جسامته، فلفظ الاعتداء ورد عامًا دون تخصيص.

فحق مؤلف برنامج الحاسب في اختيار الوقت والطريقة التي يتم بها إذاعة أو نشر برنامجه، يتمثل الاعتداء عليه عندما يذاع أو ينشر هذا البرنامج في وقت غير الوقت الذي يراه ملائمًا، أو بطريقة غير تلك التي يراها مناسبة له[2]، وقد يتخذ الاعتداء صور نقل البرنامج إلى لغة أخرى

(1) د. عبد الرازق السنهوري، الوسيط في شرح القانون المدني، دار إحياء التراث العربي، بيروت، المجلد الثامن، حق الملكية، ص 293، بند 170، نص مدني 18 فبراير 1965 مجموعة أحكام النقض من 16 ص 179 رقم 28.

(2) R. Plasisant: La loi N 85، 660 du 3 juillet 1985 relative aux droits d'auteur ètaux droits des artistes , interprétées , des producteurs de phonogrammes et de v idéogrammes et des inter prises de communications audiovisuelles , JCP , 1986 , 1 , Doct., 3230

دون ترخيص من المؤلف، كأن يترجم من لغة المصدر إلى لغة الهدف أي إلى لغة الآلة[1].

أما التحويرات الطفيفة اللازمة للاستعمال العادي للبرنامج مثل تصحيح الأخطاء، أو تحديثه أو تطويره ليؤدي الغرض الأصلي من استخدامه، فلا تدخل في نطاق التجريم، ولا يكون بالتالي التعديل أو التحوير في الحدود السابقة مكونًا لجريمة التقليد [2]، وهو ما تفرضه التشريعات والأصول الفنية والعلمية[3].

وتتوافر الجريمة سواء تم نسخ البرنامج باسم مؤلفه الحقيقي، أم باسم شخص آخر يخلق في الذهن لبسًا حول مؤلفه الحقيقي[4]، أم باسم الجاني نفسه، أم باسم صوري، ويخضع تقدير وجود التقليد ومدى الشبه أو الخلاف

(1) د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص142.

(2) Merle et vitu: Traite de droit criminal < Cujas , Paris , 1982 P. 85. T. corr. Paris , 8 kuillet 1987. Expertise , 1987 , N 98 , P 323 , obervations bloch.

وفي هذا الحكم لم تعتبر المحكمة أن الاعتداء قد وقع عن طريق النسخ غير المشروع فقط، وإنما بسبب تعطيل جهاز الأمن الذي يحول دون النسخ غير المشروع.

(3) راجع حول ذلك: د. عبد الرازق السنهوري، الوسيط في شرح القانون المدني، مرجع سابق، ص 417، د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص 126، 130، وقد ورد في مشروع تعديل قانون حماية حق المؤلف رقم 254 لسنة 1954 ومذكرته الإيضاحية إضافة فقرة أولى وهي المتعلقة بحق المؤلف في التعديل أو التحوير، ولكن هذه الفقرة لم تظهر في القانون رقم 38 لسنة 1992. وانظر نقض 16 يناير 1979، أحكام النقض س 2 ص 224 رقم 53.

(4) P 13، Trib. civ. Seinel 14 decombre 1955, GP. 1956،1

للسلطة التقديرية لمحكمة الموضوع دون رقابة عليها من محكمة النقض[1].

وتبدأ هذه الحماية من تاريخ الانتهاء من ابتكار البرنامج أو قاعدة البيانات[2]، أو من تاريخ النشر أو التوزيع أو إتاحتها للجمهور لأول مرة أيهما أبعد[3].

وتقع جريمة التقليد حتى ولو ترجم الفاعل البرنامج إلى لغات أخرى طالما أن مالك البرنامج لم يتنازل عن حقوقه أو بعضها على البرنامج، ويعتبر من قبيل التقليد المجرم قانونًا الاستعمال غير المسموح به للبرنامج، أو ما يسمى تجاوزًا بسرقة المنفعة، وبيع برنامج مقلد أو استيراده أو تصديره أو إفشاؤه أو تسويقه، أو فك شفرة البرنامج[4].

---

(1) د. محمد حسام لطفي، الحماية القانونية لبرامج الحاسب الآلي، مرجع سابق، ص 134، نقض جنائي، نوفمبر 1988، الطعن رقم 3895، س 58.

(2) د. أسامة عبد الله قايد، الحماية الجنائية لحق المؤلف، مرجع سابق، ص 143 وما بعدها.

(3) كان القانون السابق الملغي رقم 38 لسنة 1992 يضع مدة حماية خاصة لمصنفات الحاسب الآلي، فكان ينص على أن تكون هذه المدة عشرين عامًا تبدأ من تاريخ الإيداع، وبصدور القانون الجديد رقم 82 لسنة 2002 بشأن حقوق الملكية الفكرية لا توجد مدة حماية خاصة لمصنفات الحاسب الآلي.

(4) أصدرت إحدى المحاكم الفرنسية حكما انتهت فيه إلى اختلاف سرقة الكهرباء عن فك شفرة البرامج تأسيسًا على أن التيار الكهربائي ينتقل من خلال دعامة مادية يسري من خلالها، بينما فك الشفرة يتم عبر موجات الأثير اللاسلكية الهوائية أي ليس لها دعامة مادية، إلا أن محكمة استئناف باريس قد خالفت هذا الرأي وخلصت إلى أن سرقة الكهرباء وسرقة البيانات المعلوماتية تفترض وجود دعامة مادية، واعتبرت أن هذه الدعامة موجودة أيا كانت هذه الدعامة، إلا أنها خلصت لعدم انطباق جريمة السرقة على المتهم الذي قام بفك شفرة البرنامج، وبالرغم من ذلك لم تستبعد المحكمة وقوع جريمة التقليد في الدعوى المذكورة بشرط توافر الشروط الواجب توافرها مثل الجدة والأصالة إذا قام المتهم بتخزينه أو نسخه على =

3- عدم موافقة المؤلف:

يشترط لتوافر النشاط الإجرامي في جريمة التقليد إلى جانب الاعتداء على حق من حقوق المؤلف، عدم وجود إذن مسبق من المؤلف أو خلفه كتابيًا، ويشكل هذا أحد عناصر الركن المادي في الجريمة، أي أن الرضاء يعد سببًا من أسباب الإباحة، لأن المشرع في قانون حماية حق المؤلف منح المؤلف سلطة التصرف في هذا الحق ونقله إلى الغير، مما يعني أن رضاه أو إذنه يعد سببًا للإباحة[1].

وقد اشترط المشرع أن تصدر هذه الموافقة كتابة، والكتابة شرط لازم في جميع الأحوال سواء في علاقة المؤلف بالناشر أو بغيره من المتصرف إليهم سواء من العملاء أو من غيرهم، لأن النص على هذا الشرط جاء مطلقًا من كل قيد.

ومن التطبيقات القضائية الرائدة الأمر الصادر من رئيس المحكمة الابتدائية لأول درجة بباريس في 14 من أغسطس سنة 1996 والذي جاء فيه: (إن مجرد طرح المصنف الفكري للتداول عبر شبكة الإنترنت يشكل تقليدًا للمصنف ما دام أنه لا يوجد ترخيص من المؤلف صاحب الحق الاستئثاري بذلك).

وتتلخص الوقائع في أن طالبين في المدرسة الوطنية العليا للاتصالات (ENST)[2] قد أوجدا بشكل رقمي على الصفحات الخاصة بهما عبر شبكة الإنترنت مصنفًا موسيقيًا محميًا بقانون حماية حق المؤلف، وذلك دون

= دعامة جديدة.

Ca paris.24.juin 1981.gazpal.1987.2jur p.512.

(1) د. أسامة عبد الله قايد، الحماية الجنائية لحق المؤلف، مرجع سابق، ص 142.

(2) اختصارًا لـ Ecole National Superieure Des Telecommunications

تصريح من قبل الشركة المتنازل لها عن الحقوق المالية الخاصة باستغلال المصنف، الأمر الذي يعد نسخًا للمصنف، وإتاحة استعمال هذا المصنف المحمي بطريقة جماعية لكل شخص من الغير ينفذ إلى الشبكة ويزور المواقع والصفحات الخاصة بالطالبين ليتسنى له نسخ المصنف بسهولة[1].

ثانيًا: الركن المعنوي لجريمة تقليد برامج الحاسب الآلي:

جريمة التقليد عمدية يلزم لقيامها توافر القصد الجنائي بعنصريه العلم والإرادة، علم بعناصر الجريمة وإرادة متجهة إلى السلوك الإجرامي ونتيجته، وهذا هو القصد الجنائي العام الذي يكفي لتوافر الركن المعنوي[2].

وعلى ذلك فإن الركن المعنوي لجريمة التقليد يتحقق بالقصد الجنائي العام فقط لدى الجاني دون حاجة إلى لزوم توافر قصد جنائي خاص[3]، فيكفي أن يعلم الجاني أن نشاطه الإجرامي يرد على برنامج ينسب إلى شخص آخر، أي يعلم أن ما ينشره أو يذيعه أو يستعمله أو يقتبس منه من برامج يتم بدون وجه حق، وأن تتجه إرادته إلى الإذاعة أو النشر أو الاستعمال أو الاقتباس حتى يتوافر القصد الجنائي.

(1) د. أسامة أحمد بدر، بعض مشكلات تداول المصنفات عبر الإنترنت، دار النهضة العربية، 2002، ص 17.

(2) كانت المذكرة الإيضاحية للقانون المصري القديم الملغي تنص صراحة على استبعاد القصد الخاص من جريمة التقليد، حيث قررت أن القانون لم يشترط قصدًا جنائيًا، وإنما يجب توافر القصد الجنائي العام الذي يشمل بطبيعة الحال علم الجاني بتقليد المصنف، إذ إن ذلك العلم يدخل في إدراك المتهم الإجرامي المشترط في القصد الجنائي.

(3) د. عبد الرازق السنهوري، الوسيط في شرح القانون المدني، مرجع سابق، ص 434 رقم 253، د. أسامة عبد الله قايد، الحماية الجنائية لحق المؤلف، مرجع سابق، ص 152، 153.

ويتفق الفقه والقضاء الفرنسيان في أن القصد الجنائي في جريمة تقليد برامج الكمبيوتر مفترض، فإذا تحققت إحدى صور النشاط الإجرامي عد ذلك قرينة للقول بتوافر القصد الجنائي، وبمفهوم المخالفة يعني أن حسن النية لا يفترض في توافر هذه الجريمة وإن كانت هذه قرينة تقبل إثبات العكس.

وكما يوفر قانون حقوق المؤلف الحماية للمصنفات، فإنه يوفر في المقابل أيضًا مصالح الجمهور للاستفادة من هذه المصنفات، فعلى سبيل المثال تنص المادة (107) من قانون حق المؤلف الأمريكي على أن: (الاستخدام العادل لمصنف محمي بحق المؤلف، المتضمن الاستخدام بعمل نسخ منه... لأغراض مثل النقد، والتعليق، أو التقرير الإخباري، أو التدريس... الدراسة، أو البحث ليس اعتداء)[1].

الفرع الثاني

الجرائم الواردة في قانون حقوق المؤلف والحقوق المجاورة الإماراتي

نص قانون حقوق المؤلف والحقوق المجاورة رقم (7) لسنة 2002 لدولة الإمارات العربية المتحدة على أنواع مختلفة من الجرائم في المواد (37)، (38)، (39) في الفصل السابع الخاص بالإجراءات التحفظية والعقوبات.

وقد حاول المشرع في هذه المواد أن يسد الطريق أمام من يقوم بالاعتداء على المصنفات الخاصة بالمؤلفين على اختلافها، ويواجه مثل هذه الجرائم بعقوبات قد تكون صارمة وذلك على نحو ما سنرى، بعد أن نقوم بتقسيم هذه الجرائم بحسب ورودها في مواد القانون، حيث وجدنا أن

(1) برنارد أ. جالر، الملكية الفكرية وبرامج الحاسبات، مرجع سابق، ص 127.

المشرع حاول حماية المصنفات من إساءة استخدام التكنولوجيا، وبالأخص أجهزة الحاسب الآلي وشبكات الإنترنت، وشبكات المعلومات، وشبكات الاتصالات، وذلك وفقا لما يلي:

أولا: جرائم الاعتداء على حقوق المؤلف:

نص المشرع في المادة (37) من القانون على أنه: (مع عدم الإخلال بأية عقوبة أشد واردة في أي قانون آخر، يعاقب بالحبس مدة لا تقل عن شهرين، وبالغرامة التي لا تقل عن عشرة آلاف درهم ولا تزيد على خمسين ألف درهم، أو بإحدى هاتين العقوبتين، كل من قام بغير إذن كتابي من المؤلف أو صاحب الحق المجاور أو خلفهما بأي من الأفعال الآتية:

1) الاعتداء على حق من الحقوق الأدبية أو المالية للمؤلف أو صاحب الحق المجاور المنصوص عليها في هذا القانون، بما في ذلك وضع أي مصنف أو أداء أو تسجيل صوتي أو برنامج إذاعي مما تشمله الحماية المقررة في هذا القانون في متناول الجمهور، سواء عبر أجهزة الحاسب، أو شبكات الإنترنت، أو شبكات المعلومات، أو شبكات الاتصال، أو غيرها من الطرق أو الوسائل الأخرى.

2) البيع أو التأجير أو الطرح للتداول، بأية صورة من الصور لمصنف أو تسجيل صوتي أو برنامج إذاعي محمي طبقًا لأحكام هذا القانون.

وتتعدد العقوبة المنصوص عليها في هذه المادة بتعدد المصنفات أو الأداءات أو البرامج أو التسجيلات محل الجريمة.

ويعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف درهم في حالة ارتكاب الجريمة مرة أخرى.

وقد احتوت المادة سالفة البيان على صورتين من صور الاعتداء على حقوق المؤلف؛ إحداهما اعتداء مباشر على هذه الحقوق، والأخرى غير

مباشر، وسوف نبين كل صورة على حدة موضحين أركانها المادية والمعنوية، ومن ثم بيان العقوبات التي وضعها المشرع لمن يدان بارتكاب أحد هذه الأفعال.

الصورة الأولى:

جرم المشرع في هذه الصورة كافة أشكال الاعتداء على حق من الحقوق الأدبية أو المالية للمؤلف أو صاحب الحق المجاور، فتقوم الجريمة بمجرد فعل الاعتداء، وتتحقق النتيجة الإجرامية بمجرد الانتهاء من هذا الفعل، وذلك مع توافر علاقة السببية بين النشاط والنتيجة التي تحققت.

والركن المادي في جريمة الاعتداء على حق من الحقوق الأدبية والمالية للمؤلف يتمثل في قيام الجاني بأي فعل من شأنه الاعتداء على الحق الأدبي أو المالي للمؤلف، والتي سبق بيانها في المطلب السابق والمنصوص عليها في القانون.

والملاحظ على هذه المادة أن لفظ الاعتداء ورد في صيغة عامة دون تخصيص، وبالتالي فإن الجريمة تقوم أيًا كانت صورة هذا الاعتداء أو مقدار جسامته فتقوم الجريمة عند محاولة منع المؤلف من نشر المصنف، أو نسبة هذا المصنف إلى غير مؤلفه، أو قيام الغير بتعديله وتشويهه أو تحريفه إضرارًا بمكانة المؤلف.

وبالإضافة إلى حماية المشرع لهذه الحقوق الأدبية، فإنه عاقب من يقوم بالتعدي على الحقوق المالية للمؤلف، كمن يستفيد من هذا المصنف ماديًا دون موافقة المؤلف على ذلك، فالمشرع أضفى على هذه الحقوق الحماية الجنائية.

والمشرع اشترط لقيام هذه الجريمة عدم توافر إذن كتابي من المؤلف أو

صاحب الحق المجاور[1] أو خلفهما، فلو توافر هذا الإذن فلا جريمة، ويجب أن يكون هذا الإذن مكتوبًا، فلا يعتد بالإذن الشفهي إلا إذا كان له أصل مكتوب، ويجب أن يكون سابقًا على فعل الاعتداء أو معاصرًا له.

والمشرع بعد أن جرم الاعتداء على الحقوق الأدبية أو المالية للمؤلف، أورد صورة لهذا الاعتداء على سبيل المثال، وهي وضع مصنف أو أداء[2] أو تسجيل صوتي[3] أو برنامج إذاعي مما تشمله الحماية المقررة في هذا القانون في متناول الجمهور سواء عبر أجهزة الحاسب أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات، أو غيرها من الطرق أو الوسائل الأخرى.

ويتحقق الركن المادي لهذه الجريمة بوضع المصنف في متناول الجمهور، أي بنشر هذا المصنف السمعي بدون إذن كتابي من المؤلف،

---

(1) عرف القانون أصحاب الحق المجاور بأنهم فنانو الأداء، ومنتجو التسجيلات الصوتية، وهيئات الإذاعة المعرفون في هذا القانون.

(2) فنانو الأداء هم الممثلون والمغنون والموسيقيون والراقصون، وغيرهم من الأشخاص الذين يلقون أو ينشدون أو يعزفون، أو يؤدون بأية صورة، في مصنفات أدبية أو فنية أو غير ذلك محمية طبقًا لأحكام هذا القانون أو داخله في إطار الملك العام.
أما الأداء العيني فهو الأداء الذي يترتب عليه اتصال الجمهور بالمصنف اتصالا مباشرًا، كالتمثيل للمصنفات المسرحية أو التقديم أو الأداء للمصنفات الفنية، أو العرض للمصنفات السمعية البصرية، والعزف للمصنفات الموسيقية، والتلاوة للمصنفات الأدبية، ويستوي في ذلك أن يكون الأداء حيًا أو مسجلا.

(3) التسجيل الصوتي أي تثبيت يخاطب السمع لمجموعة من الأصوات لأداء معين، بغض النظر عن طريقة التثبيت، أو الدعامة المستخدمة، ويشمل التجديد الصوتي عملية تثبيت الأصوات مع الصورة لإعداد مصنف سمعي بصري ما لم يتفق على غير ذلك.

وتقوم الجريمة بالتالي بأي فعل يكون من شأنه إتاحة المصنف للجمهور بأي طريقة كانت، وذكر المشرع بعض هذه الوسائل على سبيل المثال مثل أجهزة الحاسب أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات، أو غيرها من الطرق أو الوسائل الأخرى.

والشرط الذي قرره المشرع هنا أيضًا هو عدم الموافقة الكتابية للمؤلف على هذا النشر، ويجب أن تكون هذه الموافقة سابقة على فعل النشر أو معاصرة له[1].

---

(1) ومن التطبيقات القضائية المتعلقة بشبكة الإنترنت, والتي صدرت تطبيقا لأحكام هذا القانون، قضية استعمال شعار اجتماعات صندوق النقد الدولي بدبي, حيث تتلخص القضية في قيام رئيس اللجنة المنظمة لاجتماعات صندوق النقد الدولي بدبي بإبلاغ الشرطة بقيام أحد الأشخاص [المتهم] بصفته المدير التنفيذي لإحدى الشركات بغير وجه حق، باستعمال شعار (دبي 2003) والخاص باجتماعات صندوق النقد الدولي والمسجل كعلامة تجارية مسجلة رسميا لدى وزارة المالية والصناعة، وكمصنف أدبي لدى وزارة الإعلام والثقافة، ونشره بوضعه على الموقع الإلكتروني لشركته على شبكة الإنترنت, وتم إحالة المتهم من النيابة العامة إلى المحكمة بتهمتين؛ الأولى: استعمال علامة تجارية غير قابلة للتسجيل مملوكة لحكومة دبي وهي شعار (دبي 2003)، وذلك بأن قام بوضعها على الموقع الخاص به على شبكة الإنترنت، والتهمة الثانية أنه اعتدى على حق من الحقوق الأدبية والخاصة باللجنة المنظمة لصندوق النقد الدولي، وذلك بأن وضع مصنف اللجنة والذي هو عبارة عن موقعها على شبكة الإنترنت والذي يحوي شعار (دبي 2003) على موقعه على شبكة الإنترنت بغير إذن كتابي من صاحب الحق, وطلبت النيابة العامة معاقبة المتهم طبقا لقانون العلامات التجارية الاتحادي رقم [37] لسنة 1992 المعدل بالقانون الاتحادي رقم (8) لسنة 2002، وبالمادتين (9/2، 37/1) من القانون الاتحادي رقم (7) لسنة 2002 في شأن حقوق المؤلف والحقوق المجاورة, وقد أدانته المحكمة بالتهم السابق بيانها، وقررت أن فعل المتهم يعد اعتداءً على حقوق المؤلف، وقررت تغريمه خمسة آلاف درهم. =

ولعل هذا الشرط يطرح تساؤلا حول سابقة الحصول على إذن المؤلف هل يعد سببًا من أسباب الإباحة وفقا للقواعد العامة في قانون العقوبات، أم أنه مجرد شرط لتوافر أركان الجريمة.

وقد انقسم الفقه إلى رأيين إزاء الإجابة على هذا التساؤل، ففي الوقت الذي يرى فيه البعض أن تخلف هذا الشرط تخلف للركن المادي لهذه الجريمة، وبالتالي تنتفي الجريمة كلية لانتفاء أركانها[1]، يعارض البعض الآخر هذا القول ويرون أن تخلف هذا الشرط يعد سببًا من أسباب الإباحة، وذلك على اعتبار أن المشرع على التفصيل السابق بيانه قد منح للمؤلف سلطة التصرف في هذا الحق ونقله إلى الغير، ويترتب على ذلك أن إذن المؤلف أو رضاه يعد سببًا لإباحة الأفعال السابقة وليس مجرد شرط لقيام الجريمة.

وتثير أفعال الاعتداء على الحقوق الأدبية والمالية للمؤلف عدة تساؤلات، لعل منها مدى اعتبار المؤلف مرتكبًا لجريمة الاعتداء المنصوص عليها في هذا القانون إذا ما تنازل عن حق الاستغلال أو النشر للغير ثم تصرف فيه إلى شخص آخر، فهل يتصور أن يكون المؤلف متهمًا بارتكاب جريمة اعتداء على حقوق المؤلف بعد التصرف في حقوق استغلال مصنفه إذا استغلها مرة ثانية؟

ولعلّ الذي يثير هذا التساؤل ما قررته المادة (9) من القانون حينما أجازت للمؤلف وخلفه أن ينقل إلى الغير كل أو بعض حقوقه المالية المبينة في هذا القانون.

كما أن المادة (10) أجازت للمؤلف أن يتقاضى المقابل النقدي أو العيني

= القضية رقم 7396 /2003، جزاء دبي، والحكم صادر بجلسة 2003/11/16

(1) عفيفي كامل عفيفي، جرائم الكمبيوتر، مرجع سابق، ص 64.

نظير نقل حق أو أكثر من حقوق الاستغلال المالي للمصنف إلى الغير.

ولما كانت هذه المسألة محل خلاف في الفقه فإننا نؤيد الرأي القائل بأن تصرف المؤلف في حقوقه المالية بعد نقلها إلى الغير لا يشكل جريمة تقليد، وإنما يعد فعله اعتداءً على حقوق الغير المالية تأسيسًا على أن تنازله عن حق الاستغلال لا يترتب عليه تنازله عن حقوقه الأدبية على مصنفه، بمعنى أنه لا يسقط حقه في استغلال مؤلفه، ولا يجرده من هذا الحق المقرر له وحده، فإذا خرج عن حدود استعماله لهذا الحق عدّ مخلا بشروط العقد المبرم بينه وبين الغير مما يستوجب التعويض المدني، وحكمه في ذلك حكم المؤلف الشريك في التأليف الذي يقوم بنشر مؤلف مشترك بينه وبين أكثر من شخص دون إذن منهم، فهل يسأل عن جريمة اعتداء على حق المؤلف المقرر قانونًا؟ الإجابة بالتأكيد ستكون أنه لا يسأل عن هذه الجريمة، ولكن مسئوليته فقط مسئولية مدنية تتمثل في تجاوز استعمال حقه.

وفي هذا المجال نجد سؤالا آخر يطرح نفسه، ألا وهو: هل هناك فرق بين تقليد المصنف وانتحال أو سرقة أفكار الغير؟

لما كانت القاعدة التي من أجلها صدر القانون الذي نحن بصدده هي أن حماية حق المؤلف تنصب على المصنف ذاته وليس على ما يتضمنه من أفكار، فالأفكار ليست ملكًا للمؤلف أو حكرًا عليه، ولذلك فإنه لا عقاب من الناحية الجنائية على من يعتدي على أفكار الغير، وبالتالي فإن نقل الأفكار بتصرف لا عقاب عليه، خاصة وأنه من الناحية العملية يصعب علينا أن نميز بين التقليد الجزئي ونقل الأفكار أو سرقتها، ولو أردنا ذلك لتطلب منا مجهودًا كبيرًا يتمثل في التحليل الدقيق لكل المصنفات والمقارنة بينها، خاصة وأن التقليد يكون بقدر التشابه بين المصنفين.

والركن المعنوي الواجب توافره في هذه الجريمة هو صورة القصد

الجنائي العام، والذي يقوم على العلم والإرادة، فيكفي علم الجاني بعناصر الركن المادي وأنه يقوم بفعل الاعتداء على الحقوق المالية أو الأدبية لهذا المؤلف، وأن تتجه إرادته إلى هذا الفعل، وقد كان ذلك واضحًا من سياق نص المادة (37) حيث إن ألفاظها وعباراتها لم تنص صراحة أو ضمنًا على وجوب توافر نية خاصة لدى الجاني.

والعقوبات التي وضعها المشرع لهذه الجريمة هي الحبس مدة لا تقل عن شهرين، والغرامة التي لا تقل عن عشرة آلاف درهم ولا تزيد على خمسين ألف درهم، أو إحدى هاتين العقوبتين، على أن تتعدد العقوبة بتعدد المصنفات أو الأداءات أو البرامج أو التسجيلات محل الجريمة، وفي حالة العود تكون العقوبة الحبس مدة لا تقل عن ستة أشهر، والغرامة التي لا تقل عن خمسين ألف درهم.

الصورة الثانية:

في هذه الصورة والتي وردت في المادة (37) فقرة (ب) جرم المشرع صورة أخرى من صور الاعتداء على حقوق المؤلف، وتتمثل هذه الصورة في البيع أو التأجير أو الطرح للتداول، بأية صورة من الصور لمصنف أو تسجيل صوتي أو برنامج إذاعي محمي طبقًا لأحكام هذا القانون.

والركن المادي في هذه الجريمة يتمثل في إتيان الجاني أحد الأفعال المبينة في المادة (البيع، التأجير، الطرح للتداول)، وتتحقق النتيجة الإجرامية بمجرد الانتهاء من أي فعل من هذه الأفعال، ويشترط توافر علاقة السببية بين الفعل والنتيجة التي تحققت.

ومحل الجريمة هنا هو ذلك المصنف المحمي وفقا لأحكام هذا القانون، والذي سبق الإشارة إليه.

وتعتبر الصور الواردة في هذه المادة من صور الاعتداء غير المباشر

على حقوق المؤلف، فالجاني لم يرتكب فعلا ماديًا مكونًا لجريمة التقليد، وإنما يقوم ببيع المصنف في الحالة الأولى، وتأجيره في الحالة الثانية[1]، وطرحه للتداول في الثالثة.

وتتمثل أفعال الاعتداء كما أشرنا في هذه الجريمة في التعامل في مصنفات المؤلف المحمية طبقا لأحكام القانون بدون إذن من هذا المؤلف، سواء أكان هذا التعامل بيعًا أو تأجيرًا أو تداولا بأي صورة كانت، والبيع المجرم هنا هو الذي يتم بمقتضاه نقل حق استغلال المصنف مقابل ثمن معين، ولذلك فإنه يكفي القيام بعملية البيع مرة واحدة دونما حاجة إلى تكرار مثل هذه العملية أكثر من مرة، وأما الإيجار فإنه يعني تمكين مستأجر المصنف من استعماله مدة معينة مقابل أجرة معينة، وبالمثل فإنه يكفي القيام بعملية استئجار واحدة لتوافر هذه الجريمة، وأما التداول فيقصد به التصرف في المصنف بمقابل أو بغير مقابل سواء أكان التصرف ناقلا للملكية أو غير ناقل للملكية أو أي حق آخر كحق الاستغلال أو الانتفاع[2].

واشترط المشرع في هذه الصورة من صور الاعتداء على حق المؤلف أيضًا عدم موافقة هذا المؤلف على عمليات البيع أو التأجير أو التداول، واشترط أن تكون هذه الموافقة مكتوبة وسابقة على هذه العمليات ومعاصرة لها، ويجب أن يكون التصرف في حدود هذه الموافقة، فإذا ما تم تجاوز هذه الموافقة عدّ المتجاوز مرتكبًا للجريمة السابق بيانها.

وهنا يثور تساؤل حول العرض للبيع أو التأجير هل تقوم به الجريمة؟

لما كانت هذه المسألة هي الأخرى من المسائل الخلافية في الفقه فإن

---

(1) خاطر لطفي، الموسوعة الشاملة في قوانين حماية حق المؤلف والرقابة على المصنفات الفنية، مرجع سابق، ص 175.

(2) محمد علي العريان، الجرائم المعلوماتية، مرجع سابق، ص 182.

المشرع سدّ الطريق عندما نص على عبارة (أو الطرح للتداول بأي صورة من الصور)، ولعل هذا اللفظ يشمل العرض للبيع أو التأجير، ذلك أن كل ما يصلح أن يكون محلا للبيع أو التأجير يصلح أن يكون موضوعًا للعرض للبيع أو التأجير، باعتبار أن الغاية من هذا العرض هو البيع أو التأجير، ومن ثم فإن عرض المصنف للبيع يشكل جريمة.

والركن المعنوي المطلوب توافره هنا هو القصد الجنائي العام المتمثل في العلم والإرادة، فيكفي علم الجاني بأن ما يقوم به من فعل بيع أو تأجير أو طرح للتداول اعتداء على مصنف محمي، وأن تتجه إرادته إلى فعل ذلك[1].

ثانيًا: الجرائم الأخرى المماثلة لجرائم الاعتداء:

نصت المادة (38) من قانون حقوق المؤلف والحقوق المجاورة على عدة صور لجرائم تمثل اعتداءً على حقوق المؤلف، حيث قررت أنه:

(مع عدم الإخلال بأية عقوبة أشد واردة في أي قانون آخر، يعاقب بالحبس لمدة لا تقل عن ثلاثة أشهر، وبالغرامة التي لا تقل عن خمسين ألف درهم ولا تزيد على خمسمائة ألف درهم من ارتكب أيًّا من الأفعال الآتية:

1) التصنيع أو الاستيراد دون وجه حق بغرض البيع أو التأجير أو التداول لأي مصنف أو نسخ مقلدة، أو لأية أجهزة أو وسائل أو أدوات مصممة أو معدة خصيصًا للتحايل على الحماية أو التقنية التي يستخدمها المؤلف أو صاحب الحق المجاور لبث أو طرح للتداول أو لتنظيم أو إدارة هذه الحقوق أو المحافظة على جودة نقاء معينة للنسخ.

2) التعطيل أو التعييب دون وجه حق لأي حماية تقنية أو معلومات

---

(1) نص القانون المصري بشأن حماية حقوق الملكية الفكرية رقم (82) لسنة 2002 في المادة (181) منه على الجرائم المتصور وقوعها على حق المؤلف.

إلكترونية تستهدف تنظيم وإدارة الحقوق المقررة في هذا القانون.

3) تحميل أو تخزين الحاسب بأية نسخة من برامج الحاسب أو تطبيقاته أو قواعد البيانات دون ترخيص من المؤلف أو صاحب الحق أو خلفهما.

ويعاقب بالحبس مدة لا تقل عن تسعة أشهر، وبغرامة لا تقل عن مائتي ألف درهم في حالة ارتكاب الجريمة مرة أخرى].

كما جاءت المادة (29) من هذا القانون بصورة أخرى حينما نصت على أنه:

(استثناء من حكم المادة (37) من هذا القانون يعاقب كل شخص استخدم برنامجًا للحاسب أو تطبيقاته أو قواعد البيانات دون ترخيص مسبق من المؤلف أو من يخلفه بالغرامة التي لا تقل عن عشرة آلاف درهم ولا تزيد على ثلاثين ألف درهم، لكل برنامج أو تطبيق أو قاعدة بيانات، ويعاقب بغرامة لا تقل عن ثلاثين ألف درهم في حالة ارتكاب الجريمة مرة أخرى، ويجوز للمحكمة إذا ارتكبت الجريمة باسم أو لحساب شخص اعتباري أو منشأة تجارية أو مهنية أن تقضي بالغلق لمدة لا تجاوز ثلاثة أشهر).

وسوف نتناول كل جريمة من هذه الجرائم الواردة في المادتين على حدة:

أ - جريمة التصنيع أو الاستيراد لمصنف مقلد أو لأجهزة تحايل:

جرم المشرع في الفقرة (1) من المادة (38) التصنيع أو الاستيراد دون وجه حق وبغرض البيع أو التأجير أو التداول لأي مصنف أو نسخ مقلدة، أو لأية أجهزة أو وسائل أو أدوات مصممة أو معدة خصيصًا للتحايل على الحماية أو التقنية التي يستخدمها المؤلف أو صاحب الحق المجاور لبث أو طرح للتداول أو لتنظيم أو إدارة هذه الحقوق أو المحافظة على جودة نقاء

معينة للنسخ.

فالمشرع في هذه الفقرة جرم تصنيع أو استيراد أي مصنف أو نسخ مقلدة، وهنا تناول صورة من صور تقليد المصنفات، ثم جرم أيضًا تصنيع أو استيراد أية أجهزة من شأنها التحايل على حماية المؤلف لمصنفه.

ومحل الجريمة هنا هو أي مصنف أو نسخ مقلدة، أو أي جهاز أو وسيلة أو أداة مصممة أو معدة خصيصا للتحايل على الحماية التي وضعها المؤلف.

والتقليد يعني محاكاة برنامج بصنع أو إنتاج نسخ على مثاله، بحيث تبدو عند تسويقها كالأصل، والنسخ الجزئي للبرنامج كافٍ للقول بتقليده ما دامت المحاكاة تتعلق بأجزائه الرئيسية[1].

ويتحقق فعل التصنيع بكل عمل من شأنه أن يؤدي إلى عمل مصنف أو نسخ مقلدة، أو عمل أجهزة أو وسيلة أو أداة يتم تصميمها وإعدادها من أجل الاحتيال على الحماية أو التقنية المستخدمة من قبل المؤلف.

أما الاستيراد فيتحقق بكل فعل من شأنه عبور هذه المصنفات أو النسخ المقلدة أو الأجهزة أو الوسائل أو الأدوات المعدة للاحتيال حدود الدولة السياسية قادمة من الخارج، سواء تم ذلك العبور بطريق البر أو البحر أو الجو، وسواء كان بصحبة الجاني أو بالبريد أو الشحن لحسابه، والمشرع يعاقب على الاستيراد كسلوك مجرم في ذاته حتى ولو لم يتم الهدف الذي من أجله تم الاستيراد، وهو في هذه الحالة البيع أو التأجير من أجل التحايل على حماية تقنية مستخدمة من قبل المؤلف كالتشفير أو غيره[2].

واشترط المشرع لقيام هذه الجريمة شرطين: الأول أن يتم هذا التصنيع

(1) محمد علي العريان، الجرائم المعلوماتية، مرجع سابق، ص 190.
(2) المرجع السابق، ص 190.

أو الاستيراد بدون وجه حق، ولا ندري أي وجه حق قد يتصور في حالة استيراد أو تصنيع المصنفات أو النسخ المقلدة، ونعتقد أن في هذه العبارة نوعًا من التزيد من قبل المشرع.

والشرط الثاني أن يكون هذا التصنيع أو الاستيراد قد تم بغرض البيع أو التأجير أو التداول، فإذا ما تم التصنيع أو الاستيراد لغرض آخر كالاستخدام الشخصي مثلا فلا جريمة في الأمر.

والركن المعنوي المطلوب توافره هو القصد الجنائي بنوعيه العام والخاص، فالأول مكون من العلم والإرادة، فيكفي علم الجاني بأنه يصنع أو يستورد مصنفات أو نسخًا مقلدة، أو أجهزة أو وسائل أو أدوات من أجل الاحتيال على الحماية أو التقنية المستخدمة من قبل المؤلف، وأن تتجه إرادة الجاني إلى ذلك، كما يجب توافر قصد جنائي خاص وهو غرض البيع أو التأجير أو التداول من هذا الاستيراد أو التصنيع.

ب - جريمة التعطيل أو التعييب للحماية:

الفقرة الثانية من المادة (38) جرمت التعطيل أو التعييب دون وجه حق لأي حماية تقنية أو معلومات إلكترونية تستهدف تنظيم وإدارة الحقوق المقررة في هذا القانون.

فإذا كان المشرع في الفقرة الأولى من المادة المذكورة قد جرم التصنيع أو استيراد أية أجهزة أو وسائل أو أدوات مصممة أو معدة للتحايل على الحماية أو التقنية الخاصة بالمؤلف، فقد جاء هنا وجرم استخدام مثل هذه الأدوات والأجهزة والتي قد ينجم عنها تعطيل أو تعييب هذه الحماية التقنية التي وضعها المؤلف أو المعلومات الإلكترونية، وذلك على اعتبار أن أغلب المصنفات أصبحت تعتمد على المعلومات الإلكترونية والتكنولوجيا الحديثة.

والركن المادي في هذه الجريمة يتحقق بكل فعل من شأنه أن يؤدي إلى التعطيل أو التعييب للحماية التقنية أو المعلومات الإلكترونية.

فالتعطيل والتعييب يتحققان بكل سلوك غير مشروع يأتيه الجاني على نحو يؤدي إلى

عدم تمكين الحماية التقنية من أداء وظيفتها بأي طريقة كانت، وسواء أكان التعييب جسيمًا أو غير جسيم، وبغض النظر عن الوسيلة المستخدمة طالما أنها قد أدت إلى وقوع الضرر، ويجب أن تتجه إرادة الجاني إلى هذه الأفعال بحيث يؤدي ذلك إلى إلحاق الأضرار بحماية التقنية المستخدمة من قبل المؤلف، وتجدر الإشارة إلى أن هذه الجريمة تعتبر جريمة مادية أي جريمة ضرر، ومن ثم يتعين أن يترتب على سلوك الجاني حدوث التعطيل أو التعييب لحماية التقنية المستخدمة من المؤلف[1].

والقصد الجنائي هنا هو القصد العام، فيكفي علم الجاني بأن ما يقوم به يعد من أفعال الاعتداء على حماية تقنية أو معلومات إلكترونية مستخدمة من قبل المؤلف، وأن تتجه إرادته إلى هذا السلوك غير المشروع المتمثل في التعطيل أو التعييب.

ج - جريمة تحميل الحاسب ببرنامج غير مرخص:

في الفقرة الثالثة من هذه المادة نص المشرع على حماية خاصة لبرامج الحاسب الآلي، فجرم تحميل أو تخزين الحاسب بأية نسخة من برامج الحاسب أو تطبيقاته أو قواعد البيانات دون ترخيص من المؤلف أو صاحب الحق أو خلفهما.

ومحل الجريمة هنا هو برنامج الحاسب الآلي أو تطبيقاته أو قواعد البيانات، إذا ما قام الجاني بتحميلها أو تخزينها على الحاسب بدون ترخيص من المؤلف أو صاحب الحق أو خلفهما.

(1) محمد علي العريان، الجرائم المعلوماتية، مرجع سابق، ص 191.

وتقوم الجريمة هنا بمجرد القيام بتحميل وتخزين الحاسب بهذا البرنامج بدون ترخيص من المؤلف، ولم يشترط المشرع أن تكون موافقة المؤلف مكتوبة هنا، وإنما يكفي ترخيص هذا المؤلف بالسماح بتحميل أو تخزين هذا البرنامج الخاص به، ويتحقق ذلك من خلال شراء النسخة الأصلية من هذا البرنامج والذي طرحه المؤلف في السوق.

وهذا النص جاء لوضع حد للخلاف الذي كان مثارًا في ظل قانون حماية المصنفات الفكرية وحقوق المؤلف رقم (40) لسنة 1992 والذي كان معمولا به قبل تطبيق هذا القانون الذي نحن بصدده، حيث إن القانون السابق لم ينص صراحة على تحميل الكمبيوتر ببرنامج دون ترخيص من المؤلف، الأمر الذي أدى إلى قيام المحاكم بتبرئة المتهمين في مثل هذه القضايا تطبيقًا لمبدأ الشرعية.

وتحميل الكمبيوتر بالبرنامج يعني نسخ هذا البرنامج من شريط أو قرص إلى ذاكرة الحاسب، والطريقة المتبعة عند شراء برنامج حاسب هي أن يحدد مالك المصنف [البرنامج] في اتفاقية الترخيص التي تعطى للمشتري مع هذا المصنف الشروط التي يجب أن يلتزم بها المستخدم، ومنها أن يستخدم هذا البرنامج على جهاز كمبيوتر واحد دون أن يتعداه إلى عدة أجهزة؛ لأن في ذلك مخالفة لشروط الترخيص، وبالتالي تقوم الجريمة الواردة في هذه الفقرة، ومع العلم أنه في بعض الأحيان يتم منح رخصة جماعية لاستخدام البرنامج وهي عادة تمنح للمؤسسات الكبيرة والشركات.

والشرط الوحيد الذي اشترطه المشرع هنا لقيام الجريمة هو عدم الحصول على ترخيص بهذا التخزين والتحميل من المؤلف صاحب البرنامج، ولم يشترط المشرع أن يكون هذا الترخيص مكتوبًا، فيكفي ترخيص المؤلف بأية صورة تنم عن موافقته بالقيام بتخزين أو تحميل

برنامجه على الحاسب، وذلك على العكس مما قرره المشرع المصري عندما اشترط أن تكون الموافقة مكتوبة.

والركن المعنوي المتطلب توافره هنا هو القصد الجنائي العام المتمثل في علم الجاني بأن ما يقوم به من فعل تخزين أو تحميل الحاسب ببرنامج دون الحصول على تصريح من صاحب هذا البرنامج، ويجب أن تتجه إرادة الجاني إلى إحداث هذا الفعل.

والعقوبات التي قررها المشرع للصور الثلاثة السابقة من جرائم الاعتداء على حقوق المؤلف هي الجمع بين عقوبة الحبس لمدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن خمسين ألف درهم ولا تزيد عن خمسمائة ألف درهم، وفي حالة العود تكون العقوبة الحبس مدة لا تقل عن تسعة أشهر والغرامة التي لا تقل عن مائتي ألف درهم.

د - جريمة استخدام برنامج دون ترخيص:

ما سبق وأن ذكرناه أثناء حديثنا عن جريمة تحميل أو تخزين الحاسب الآلي ببرنامج دون ترخيص مؤلفه ينطبق على هذه الجريمة، ولكن الفرق أن المشرع في الجريمة السابقة عاقب على فعل التحميل والتخزين في الحاسب الآلي دون ترخيص من المؤلف، ولكن في هذه الجريمة نجد أن المشرع عاقب على فعل الاستخدام لبرنامج حاسب أو تطبيقاته أو قواعد البيانات دون ترخيص مسبق من المؤلف.

ومحل الجريمة هنا هو برنامج الحاسب أو تطبيقات هذا البرنامج أو قاعدة البيانات إذا ما تم استخدامها بدون ترخيص مسبق من المؤلف.

وتقوم الجريمة بفعل الاستخدام فقط دون انتظار حصول نتيجة معينة من جراء هذا الاستخدام.

واشترط المشرع لقيام الجريمة هنا عدم الحصول على ترخيص من

المؤلف بهذا الاستخدام، ولم يشترط أن يكون هذا الترخيص مكتوبًا، وإنما يجب أن يكون سابقًا على فعل الاستخدام.

والركن المعنوي في هذه الجريمة هو القصد الجنائي العام المتمثل في علم الجاني باستخدامه لبرنامج دون ترخيص من مؤلفه، واتجاه إرادته إلى هذا الفعل.

والعقوبات التي وضعها المشرع لهذه الجريمة هي الغرامة التي لا تقل عن عشرة آلاف درهم ولا تزيد على ثلاثين ألف درهم، وتتعدد العقوبة بتعدد البرامج أو التطبيقات أو قواعد البيانات، والعقوبة في حالة العود هي الغرامة التي لا تقل عن ثلاثين ألف درهم، وأجاز المشرع للمحكمة إذا ارتكبت الجريمة باسم أو لحساب شخص اعتباري أو منشأة تجارية أو مهنية أن تقضي بالغلق لمدة لا تجاوز ثلاث شهور.

وأخيرًا فإننا نعتقد أن قانون حماية المؤلف والحقوق المجاورة قد جاء بشكل رئيسي لمواجهة الاعتداء على حقوق المؤلف من خلال شبكة الإنترنت ووسائل الاتصال والتكنولوجيا الحديثة، وليس أدل على ذلك من أنه في مواد العقوبات، والتي سبق بيانها تفصيلا جعل الحماية القانونية لحقوق المؤلفين عن طريق حماية المصنفات من الانتهاك عبر أجهزة الحاسب أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصالات أو غيرها من الطرق أو الوسائل الأخرى، فاعتبر شبكة الإنترنت وما شابهها من وسائل الاتصال هي الأصل في موضوع الحماية، ثم حمل عليها الطرق أو الوسائل الأخرى.

كما قام القانون ببسط الحماية الجنائية على الحماية التقنية أو المعلومات الإلكترونية التي يستخدمها المؤلف لحماية مصنفه، وأضفى أيضًا هذه الحماية على برامج الحاسب، وعاقب على تحميلها وتخزينها أو استخدامها

بدون ترخيص مسبق من المؤلف، سواء أكانت برامج للحاسب أو تطبيقاته أو قواعد البيانات، وفي ظل وجود مثل هذا القانون نستطيع القول أيضًا بأنه يعد مرتكبًا لجريمة اعتداء على حق المؤلف من يقوم بتقليد موقع للإنترنت أو التعديل أو التحوير فيه دون موافقة صاحبه[1].



(1) د. مدحت عبد الحليم رمضان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 65.

المبحث الثالث

الاعتداء على العلامة التجارية عبر شبكة الإنترنت

تعرف اتفاقية الجوانب المتصلة بالتجارة لحقوق الملكية الفكرية (تربس) العلامة التجارية[1] بأنها أي إشارة أو مجموعة إشارات تسمح بتمييز السلع أو الخدمات التي تنتجها منشأة ما عن تلك التي تنتجها المنشآت الأخرى صالحة لأن تكون علامة تجارية، وتكون هذه العلامات لاسيما الكلمات التي تشمل أسماءً وحروفًا وأرقامًا للتسجيل كعلامات تجارية، وحين لا يكون في هذه العلامات ما يسمح بتمييز السلع والخدمات ذات الصلة يجوز للبلدان الأعضاء أن تجعل الصلاحية للتسجيل مشروطة بالتمييز المكتسب من خلال الاستخدام، كما يجوز لها اشتراط أن تكون العلامات المزمع تسجيلها قابلة للإدراك بالنظر كشرط لتسجيلها.

وبذلك فإن اتفاقية تربس قد تضمنت تعريفًا واسعًا للعلامة التجارية، ونظرًا لما حظيت به هذه الاتفاقية من الاعتراف الدولي الواسع، فإن ذلك سيؤدي إلى توحيد مفهوم العلامة التجارية دوليًا، ومع ذلك يختلف تعريف العلامات التجارية طبقًا للتشريعات الوطنية أو الاتفاقيات الدولية التي تنص على الحماية القانونية للعلامات التجارية.

وقد عرف قانون العلامات التجارية الإماراتي[2] العلامة التجارية بقوله: (تعتبر علامة تجارية كل ما يأخذ شكلا مميزاً من أسماء أو كلمات أو إمضاءات أو حروف أو أرقام أو رسوم أو رموز أو عناوين أو دمغات أو

(1) وفقا للمادة 1/15 من اتفاقية تربس.

(2) وفقا للمادة (2) من القانون الاتحادي رقم (37) لسنة 1992م في شأن العلامات التجارية.

أختام أو صور أو نقوش أو إعلانات أو عبوات، أو أية علامة أخرى، أو أي مجموع منها، إذا كانت تستخدم أو يراد أن تستخدم إما في تمييز بضائع أو منتجات أو خدمات، أيًّا كان مصدرها، وإما للدلالة على أن البضائع أو المنتجات تعود لمالك العلامة بسبب صنعها أو انتقائها أو الاتجار بها، أو للدلالة على تأدية خدمة من الخدمات، ويعتبر الصوت جزءًا من العلامة التجارية إذا كان مصاحبًا لها).

وتثور المنازعات بين مالك العلامة التجارية وبين صاحب اسم الحقل متى كان اسم الحقل أو جزء أساسي منه بمثابة نسخة أو تقليد أو نقل حرفي أو ترجمة للعلامة شائعة الشهرة وتم تسجيله أو الانتفاع به عن سوء نية؛ لأن هذا التسجيل يحرم الغير وبشكل نهائي من إمكانية الحصول على العنوان نفسه في المجال نفسه وفي كل دول العالم ولأي منتج، ويؤدي ذلك بطبيعة الحال إلى إثارة المشكلات بين مسجلي أسماء الحقول ومالكي العلامات التجارية الذين قد يرغبون في تسجيل أسماء حقل تمثل علاماتهم التجارية[1].

وقد يعمد صاحب اسم الحقل إلى تسجيل هذا الاسم بهدف إعادة بيعه مرة أخرى بثمن مغالى فيه إلى مالك العلامة الأصلية أو لأحد منافسيه، ويمثل هذا الاعتداء نوعًا من القرصنة أو السطو الإلكتروني على العلامات المملوكة للآخرين.

وقد ارتبط ظهور هذه الصورة من صور القرصنة الإلكترونية بظهور شبكة الإنترنت كوسيلة اتصال عالمية وسريعة، وارتبط ظهورها أيضًا بالفكرة السائدة لدى الأغلبية بأن شبكة الإنترنت فضاء لا يحكمه قانون،

(1) د. شريف محمد غانم، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار النهضة العربية، ص 101.

لذلك تناولنا هذا المبحث وفق المطالب التالية:

المطلب الأول: المقصود بالسطو على أسماء الحقول

المطلب الثاني: العوامل المشجعة على السطو الإلكتروني

المطلب الثالث: صور السطو الإلكتروني

المطلب الأول

المقصود بالسطو على أسماء الحقول

تتعدد أساليب الاعتداء على أسماء الحقول من قبل قراصنة شبكة الإنترنت، والشكل الأكثر شيوعًا لهذه الأساليب هو قيام بعض الأشخاص بتسجيل أسماء حقول بشكل قانوني لدى الجهة المختصة، وتضمين اسم الحقل إحدى العلامات التجارية المسجلة بشكل مسبق، ويكون الغرض من هذا التسجيل اكتساب ملكية اسم الحقل لإعادة بيعه إلى المالكين الأصليين للعلامة التجارية بعد الحصول على تعويض مالي كبير للتخلي عن ملكية اسم الحقل[1].

(1) أصبح اختيار اسم الحقل قرارًا مهما بالنسبة للشركات, واسم الحقل هو الاسم الذي تسجّله لتمكين مستخدمي شبكة الإنترنت من تحديد موقع شركتك على شبكة الويب، ويمكن تسجيل أسماء الحقول في أي عدد من "الحقول العليا" (المشار إليها اختصارًا "TLD") ولك أن تختار اسمًا من الحقول العليا المكونة من أسماء عامة" مثل.com أو.net أو.org أو.info كما يمكن اختيار اسم من الحقول المخصصة والمحدودة إذا كنت مؤهلا لاستخدامها (مثل.aero لشركات الطيران والنقل الجوي أو.biz للشركات التجارية) ولك أيضا أن تسجل اسمًا ضمن فئة "الحقول العليا المكونة من رموز البلدان" (ccTLD)، مثل.bn في بلغاريا أو.cn في الصين أو.ch في سويسرا, أو ae في الإمارات.
وتعد هيئة شبكة الإنترنت المعنية بالأسماء والأرقام المعيّنة (ICANN) هي التي تدير أسماء الحقول من الناحية التقنية، أما التسجيلات في الحقول العليا المكونة =

= من أسماء عامة (gTLD) فيتولاها عدد من أمناء التسجيل على شبكة الإنترنت المعتمدين لدى هيئة شبكة الإنترنت، ويمكن الاطلاع على قائمة أمناء التسجيل في موقع الهيئة على العنوان التالي: http://www.icann.org. ويمكن التأكد من أن اسم الحقل قد سبق تسجيله بالبحث في موقع من مواقع أمناء التسجيل أو باستعمال إمكانيات البحث بنظام "Whois" كنظام البحث الذي تتيحه خدمات "Uwhois" عبر موقعها http://www.uwhois.com.

أما بالنسبة إلى التسجيلات في فئة الحقول العليا المكونة من رموز البلدان (ccTLD) فينبغي الاتصال بهيئة التسجيل المعيّنة لكل حقل أعلى مكون من رمز بلد، ويمكن لذلك الغرض البحث في قاعدة البيانات الخاصة بالحقول العليا المكونة من رموز البلدان التي وضعتها الوايبو والتي توصل إلى مواقع 243 حقلا من تلك الفئة، حيث توجد معلومات عن اتفاقيات التسجيل وخدمات "Whois" وإجراءات تسوية المنازعات, وعند اختيار اسم حقل للشركة، يمكن اختيار اسم عام أو شائع حسب مكان تسجيله، ولكن في حال اختيار اسم مميز، فقد يسهل على المستخدمين تذكّره والبحث عنه، ويستحسن أن يكون مميزا لدرجة تجعله أهلا للحماية بموجب قانون العلامات التجارية؛ لأن أسماء الحقول أهل للحماية كعلامات تجارية في بعض البلدان، فإذا اخترت اسمًا شائع الاستعمال (مثل: "برنامج ممتاز")، فستواجه صعوبة جمّة في تكوين سمعة متميّزة أو شهرة تجارية خاصة بذلك الاسم، بل وقد تواجه صعوبة أكبر في منع الغير من استعمال الاسم في الممارسات التنافسية, وينبغي ألا يكون اسم الحقل الذي تختاره علامة تجارية تملكها شركة أخرى، وخاصة ألا تكون علامة شائعة الشهرة، وتنص معظم القوانين على أن تسجيل علامة تجارية يملكها الغير كاسم حقل يعدّ تعديا على العلامة التجارية، وهو ما يعرف بعبارة "السطو الإلكتروني"، وقد تضطر شركتك إلى نقله أو شطبه ودفع تعويضات أيضا.

ثم إن أسماء الحقول المسجلة في فئة الحقول العليا المكونة من أسماء عامة (مثل .com) وعدة أسماء حقول مسجلة في فئة الحقول العليا المكونة من رموز بلدان، كلها تخضع لإجراءات تسوية المنازعات (الوارد وصفها أدناه) تتيح لمالك العلامة التجارية أو علامة الخدمة إمكانية منع السطو الإلكتروني على علاماته، وهناك عدة قواعد بيانات على الويب يمكن البحث فيها للتأكد من أن اسم الحقل الذي اخترته=

وكما يقوم القراصنة بالاعتداء على الحقول، فإنهم يقومون بالقدر نفسه بالاعتداء على البرامج، وذلك على اعتبار أن كل منهما مكمل للآخر[1].

= ليس علامة تجارية مسجلة في بلد معين، ولقد أقامت الوايبو بوابة على شبكة الإنترنت تتيح النفاذ إلى قاعدة بيانات بالعلامات التجارية للمساعدة على إجراء ذلك البحث http://ecommerce.wipo.int/databases/trademark/index.html

وداثما تتساءل الوايبو حول: ماذا تفعل إذا اكتشفت أن أحدًا آخر يستعمل العلامة التجارية أو علامة الخدمة لشركتك كاسم حقل؟ وللإجابة على هذا التساؤل تقرر أنه احترف بعض الأشخاص من عديمي الضمير ممارسة "السطو الإلكتروني"، والهدف من ذلك في الغالب هو انتزاع الأموال من المالك الشرعي للاسم أو تضليل المستهلك وإحداث اللبس لديه، وإذا اكتشفت أن العلامة التجارية أو علامة الخدمة لشركتك تتعرض للسطو الإلكتروني فلك أن تتبع إجراءات بسيطة على الشبكة، حيث يتخذ خبير مستقل قرارا يبتّ في إمكانية ردّ اسم الحقل إليك، فيكون أمناء التسجيل ملزمين باتباع ذلك القرار، وجاءت هذه الإجراءات بالسياسة الإدارية الموحدة لتسوية المنازعات (UDRP) في الأصل بناءً على اقتراح من الوايبو كنتيجة لمشروعي الوايبو الأول والثاني بشأن شبكة الإنترنت، ثم اعتمدتها هيئة شبكة الإنترنت المعنية بالأسماء والأرقام المعيّنة (ICANN). وهناك معلومات عنها في موقع الوايبو على الويب: http://arbiter.wipo.int/domains/ ، وفضلا عن العلامات التجارية، يوصى بتفادي اختيار أسماء الحقول التي تتألف من بعض الكلمات الأخرى المثيرة للجدل مثل المصطلحات الجغرافية وأسماء المشاهير وأسماء الأدوية النوعية وأسماء المنظمات الدولية والأسماء التجارية (مثل اسم مشروع تجاري لشخص آخر) والتي قد تتداخل مع حقوق الغير أو أنظمة للحماية الدولية, للمزيد يزار الموقع:

http://www.wipo.int/sme/ar/e_commerce/domain_names.htm

(1) ويعتبر المثال البارز في هذا الشأن قضية شركة (Panavision international) التي تمتلك العلامتين المشهورتين: (Panavision , Panaflex) وهاتان العلامتان استخدما بالارتباط مع عمل الشركة بالتصوير الفوتوغرافي، وفي عام 1995 سجل المدعو "Dennis toeppen" اسم حقل تحت عنوان "Panavision.com" وسجل لاحقًا اسم حقل آخر بعنوان "Panaflex.com"، وذلك قبل أن تبادر شركة =

وتعـرف قرصـنة الـبرامج بأنهـا الاعتـداء بالنسـخ أو الاسـتعمال غـير المشروع لـبرامج الكمبيـوتر، وطبقًـا لإحصـائية اتحـاد منتجـي الـبرامج لعـام 2000 تصـل نسـبة القرصـنة إلى 56 %، بيـنما تقـدر الخسـائر بــ 12 مليـون دولار[1]، وتلحـق قرصـنة الـبرامج الضرـر بكـل الشركات المنتجـة لـبرامج الكمبيـوتر، بالإضـافة إلى المسـتخدمين أنفسـهم، وهـي تـؤدي إلى ارتفـاع أسـعار الـبرامج بالنسـبة للمسـتخدمين، وإلى انحـدار مسـتوى الـدعم الفنـي للـبرامج، كـما أنهـا تتسـبب في تـأخر تمويـل عمليـات تطـوير بـرامج جديـدة، مـما يـؤدي بالتـالي إلى تدهور مستوى صناعة البرامج.

كذلك تلحق القرصنة أضرارًا بكل من ناشري وموزعي بـرامج الكمبيـوتر أيًـا كـان حجمهـم، فالمبرمجون ينفقون أعوامًا لتطوير برنامج ما، وهناك جزء من المقابـل المـالي الـذي يحصـل عليـه مطورو البرنامج يوجه إلى تطوير برامج جديدة، بحيث تستمر تلك البرامج في التطور والتقدم نحو

= "Panavision" الدولية إلى تسـجيل هـاتين العلامتـين كأسـماء حقـول عـلى شـبكة الإنترنـت، ولقـد كـان "Dennis" مقـدرًا لأهميـة التجـارة الإلكترونيـة بالكامـل أو الخطـر الـذي يمكـن أن يقـوم بـه الآخـرون باستعمال هذه العلامات كأسماء حقول، ولم يقم (Dennis) بأي عمل حقيقي لاستعمال أسماء الحقـول التي قام بتسجيلها، وطلبت شركة (Panavision) من (Dennis) التوقف عن استعمال هـذين الاسـمين، وبالمقابل طلب (Dennis) مبلغ 1300 دولار كتعويض للتوقـف عـن اسـتعمال أسـماء الحقـول الخاصـة بالعلامات التجارية (Panavision)، وقد أقامت شركة (Panavision) الدعوى ضد (Dennis) لمنع هـذا الاعتداء، وطلبت المحكمة من (Dennis) التخفيف من علامات (Panavision)، وبالرغم من ذلـك فقـد سجل (Dennis) علامات مشهورة أخرى وحاول القيام بأعمال أخرى تدخل ضمن ما يدعى الآن بقرصـنة شبكة الإنترنت.

(1) وردت هذه الأرقام بمجلة اتحاد منتجي برامج الكمبيوتر التجارية، العدد 11، ص4.

الأفضل، أما عند شراء نسخ البرامج المسروقة تذهب العائدات مباشرة إلى جيوب قراصنة البرامج.

وتسيء قرصنة البرامج إلى الاقتصاد المحلي، إذ إن انخفاض حجم مبيعات البرامج الأصلية ينتج عنه انخفاض في العائدات وازدياد في البطالة، كما تقف قرصنة البرامج عقبة في وجه تطوير صناعة برامج الكمبيوتر المحلية، فإذا لم يستطيع المبرمجون تسويق منتجاتهم تحت حماية القانون، فلن يكون لديهم الحافز للاستمرار في عمل هذه البرامج، فمن شأن الجهد الضخم الذي يتم بذله في مجال الأبحاث والتطوير والاستثمارات والتكلفة العالية التي يتطلبها تطوير البرامج، أن يتعرض صغار المبرمجين من الشركات أو الأفراد لمخاطر اقتصادية من جراء القرصنة، والمبرمجون الصغار عادة ما يكونون مصدرًا أساسيًا لأفكار إبداعية في مجال البرامج، وهي أفكار حيوية ليس فقط بالنسبة لكبرى شركات البرامج، ولكن أيضًا لاستمرار تطور مجتمع تكنولوجيا المعلومات بأسره، فالمحصلة النهائية للقرصنة هي انخفاض فرص العمل وإعاقة الإبداع في مجال صناعة البرامج، لهذا لابد أن تقوم السلطات والمؤسسات والأفراد ببذل الجهد لمكافحة القرصنة، وإيجاد قوانين ملائمة لحماية الملكية الفكرية في هذا المجال.

ويؤسس النظام القانوني لنطاق الأسماء في القانون المقارن على التشريع أساسًا في الوقت الذي يتم فيه اعتماد وثائق من مؤسسات أخرى للتنظيم, ففي الولايات المتحدة الأمريكية مثلا يحكم نظام نطاق الأسماء ما يلي:

- قانون مكافحة العدوان على نطاق الأسماء The Cybersquatting Act, وهو قانون فيدرالي صادر في 29 نوفمبر 1999, في قانون العلامات التجارية, وهو القانون الذي يتناول استخدام أو تسجيل نطاق

الأسماء والعلاقة بين ذلك ومدى حسن النية أو سوء النية في هذا الشأن, وفكرة هذا القانون مستمدة من قانون العلامات التجارية الفيدرالي The lanham Act.

- قرار الأيكان بشأن سياسة المنازعة في نطاق الأسماء UDRP الصادر في 24 أكتوبر 1999 , والمطبق منذ 1 يناير 2000, والذي يتناول بالتنظيم المستوى العالي لنطاق الأسماء مثل com و org , وغيرها[1].

ويعتبر القانون الأمريكي لحماية المستهلك الإلكتروني الصادر في عام 1999 انتهاك حقوق ملكية العلامات التجارية من خلال قرصنة شبكة الإنترنت (سواء بتسجيلها كأسماء حقول أو بتقليدها) من الأعمال غير الشرعية، ويخول القانون مالك العلامة حق إقامة دعوى مدنية لمقاضاة المعتدي على اسم الحقل باستخدام العلامة التجارية، عندما يتوافر لديه سوء النية بهدف تحقيق الربح من السطو الإلكتروني، والتدابير التي من الممكن أن تقضي بها المحكمة استنادًا إلى هذا القانون يمكن أن تتضمن إلغاء تسجيل المعتدي بالقرصنة الإلكترونية لاسم الحقل وتحويله إلى المالك الحقيقي للعلامة، والتعويض المادي عن الأضرار والأرباح التي حصل عليها من استغلال اسم الحقل، وقد تصل قيمة التعويض إلى 100.000 دولار أمريكي، وبذلك فإن أي شخص سيكون مسئولا عن استغلال العلامات التجارية بتسجيلها كأسماء حقول وفقًا لأحكام هذا القانون.

ويقصد بالقرصنة أو السطو الإلكتروني أن يقوم شخص طبيعي أو معنوي لا يمتلك أي حق على علامة تجارية بتسجيل هذه العلامة في صورة اسم حقل على شبكة الإنترنت، قاصدًا الإضرار بمالكها، أو بقصد إعادة بيع

(1) د. عمر محمد أبو بكر بن يونس, الأيكان, مرجع سابق, ص 31.

اسم الحقل إلى هذا المالك مرة أخرى، أو لأحد منافسيه بثمن مغالى فيه.

ويبيع القرصان أسماء الحقول الإلكترونية التي سجلها متعمدًا الخلط واللبس في أذهان الجمهور المتولد من اختياره العلامات التجارية المشهورة ليقوم بتسجيل أسماء حقول إلكترونية تمثلها، وهو مطمئن إلى أن مالك العلامة المشهورة حرصًا منه على سمعة علامته، سوف يسعى للتفاوض معه بهدف استرداد هذا الاسم بأي ثمن يطلبه.

وقد تنبه القضاء في أوروبا والولايات المتحدة الأمريكية منذ عام 1996 إلى خطورة هذه القرصنة، فأصدر العديد من الأحكام في هذا الإطار، ومن الأحكام القضائية التي صدرت بإدانة القرصنة أو السطو الإلكتروني ذلك الحكم الصادر من المحكمة الابتدائية لمدينة Nanterre الفرنسية عام 2000، فقد جاء في الحكم أن: "البيع بالمزاد العلني لأسماء حقول إلكترونية مقلدة لعلامات تجارية مشهورة يشكل عملا من أعمال القرصنة توجب مسئولية من اشترك فيه"[1].

ويؤسس القضاء الأحكام الصادرة بإدانة القرصنة الإلكترونية في مجملها على سوء نية من يقوم بها عند تسجيله لأسماء الحقول الإلكترونية أو عند استخدامه لها، ويستظهر القضاة سوء نية مسجل الاسم من مؤشرات عديدة، منها إعادة بيع اسم الحقل بما يدلل على سوء نية من يقوم بعملية القرصنة أو السطو الإلكتروني، ونية الإضرار بمالك العلامة التجارية؛ لأنه يتوافر سوء النية لدى مسجل اسم الحقل أيضًا إذا سجل هذا الاسم بهدف الإضرار بمالك العلامة التجارية، وذلك بمنعه من تسجيل أسماء تمثل علامته على شبكة الإنترنت، فمنع مالكي العلامات التجارية من استخدام علامتهم عبر الشبكة يمثل ضررًا كبيرًا يصيب هؤلاء الملاك ويدل بوضوح على سوء

(1) http://www.legalis.net/jnetldecisions/marques/tgi_nanterre_srf.htm

نية المسجل.

ووفقًا لقانون مكافحة العدوان على نطاق الأسماء الأمريكي ACPA فإنه يمكن لحائز نطاق الاسم رفع دعواه إلى القضاء لإعادة الاسم إليه أو منع الغير من استخدامه, وكذلك الحصول على التعويضات الملائمة إذا وجد مبرر لها في هذا الشأن, ويتطلب القانون المذكور ضرورة توافر سوء نية Bad Faith لدى المعتدي, ولكي يتم التوصل إلى سوء النية هنا فإن التشريع المذكور يقرر أنه يجب على محكمة الموضوع مراعاة ما يلي من عناصر كحد أدنى:

- ما إذا كان لدى مرتكب تسجيل العلامة أي حقوق ملكية علامة تجارية على الاسم.
- ما إذا كان لدى مرتكب تسجيل العلامة أية حقوق لبيانات اسمية على الاسم.
- ما إذا كان مرتكب التسجيل مستندًا إلى قاعدة الشفافية Faire Use أو حسن نية Bona Fide غير تجارية على نطاق الاسم.
- ما إذا كان لدى مرتكب التسجيل النية لصرف المستهلكين عن موقع حائز العلامة التجارية بقصد الحصول على مكسب مالي, أو التقليل من أهمية العلامة التجارية وخلق اضطراب وإرباك حول موقع الإنترنت.
- ما إذا كان مرتكب التسجيل قد قام بعرض أو تحويل أو بيع أو تخلى عن نطاق الاسم دون أن يقوم باستخدامه، أو كانت لديه النية في استخدام نطاق الاسم، أو ما إذا كان قد قام بسلوك ينبئ عن ذلك كله.
- ما لو كان الشخص قد قدم معلومات مزيفة أو مضللة للجهة القائمة

بالتسجيل[1].

والواقع أن ظاهرة بيع أسماء الحقول الإلكترونية بأثمان مبالغ فيها لأصحابها الحقيقيين أصبحت واقعًا لا يمكن إنكاره، بحيث يمكن القول بأنها أصبحت تشكل "سوقًا لبيع أسماء الحقول الإلكترونية" فهنالك العديد من المواقع عبر شبكة الإنترنت مختصة ببيع أسماء الحقول الإلكترونية، بحيث يكتب اسم الحقل وملحقًا به ثمنه.

وتسجل أسماء الحقول الإلكترونية ارتفاعًا ملحوظًا في أثمان هذه العناوين الإلكترونية، خاصة إذا كانت تمثل علامات دولية مشهورة[2].

ويدين القضاء القرصنة المتمثلة في العمل غير الأخلاقي الذي يقوم به من يمارس القرصنة أو السطو الإلكتروني في استغلال الأشخاص والمشروعات نظرا للقصور الذي تتضمنه قواعد تسجيل أسماء الحقول الإلكترونية، بما يؤدي إلى تسجيل عدد كبير منها للمتاجرة فيها دون أي وجه حق أو مصلحة مشروعة، فالاعتداء على أسماء الحقول، وإعادة بيعها لأصحابها، أمر يرفضه القانون ويختل به أمن المعاملات عبر شبكة الإنترنت، ولهذا السبب فإن القضاء يعتبر أن مجرد عرض اسم حقل على شبكة الإنترنت للبيع يمثل سطوًا، ويسأل من يقوم به حتى ولو لم يتم البيع بالفعل، فمجرد العرض للبيع يكشف عن سوء نية القرصان في الاستفادة من

(1) د. عمر محمد أبو بكر بن يونس, الأيكان, مرجع سابق, ص 34.

(2) وعلى سبيل المثال وصل ثمن اسم الحقل: altavisa.Com إلى 3.3 مليون دولار دفعته شركة "Compaq" لتحصل عليه لنفسها، ووصل ثمن اسم الحقل "Business.com" إلى 7.5 مليون دولار الذي اشترته شركة: companies،E، ووصل ثمن اسم الحقل: mp3audobooks.com إلى 8 مليون دولار، وثمن اسم الحقل: drugs.com إلى 800 ألف دولار.

المتاجرة في اسم الحقل.

كما يستشف القضاء نية إعادة البيع لدى مسجل اسم الحقل من ظروف الواقعة ذاتها[1]، كما أن شهرة العلامة التي يمتلكها المدعي قد تخلق في حد ذاتها قرينة بسيطة على أن مسجل اسم الحقل قد قصد من تسجيله لهذا الاسم إعادة بيعه مرة أخرى إلى مالك العلامة، فشهرة العلامة التجارية تعد دليلا في بعض الأحيان على وجود نية إعادة البيع لدى مسجل الاسم.

وتتضح نية الإضرار أكثر إذا قام القرصان بتسجيل اسم الحقل في أكثر من مجال لمنع ظهور مالك العلامة التجارية على شبكة الإنترنت، فتسجيل أحد الأشخاص لأسماء الحقول الإلكترونية يبين بوضوح نية المسجل في منع هذه الشركة من الظهور على شبكة الإنترنت، مما يدفع مالكيها للتفاوض معه أو الدخول في منازعات قضائية لاسترداد هذه الأسماء.

(1) ومن تطبيقات هذه الفكرة القرار الصادر من مركز التحكيم والوساطة التابع للمنظمة العالمية للملكية الفكرية Wipo في 13 مارس 2002 في قضية "Air France"، ففي هذه القضية توصلت اللجنة التي نظرت النزاع إلى وجود نية إعادة بيع أسماء الحقول الإلكترونية: delta.com،airfrance لدى مسجل هذه الأسماء وهي شركة "van wijk" الأمريكية من عبارة أجابت بها الشركة المدعى عليها على الشكوى المقدمة من المدعية، وتتمثل هذه العبارة في "please come with a better idea"، فقد وصفت اللجنة هذه العبارة بأنها غامضة، ويمكن تفسيرها على الأرجح بأنه دعوى من المدعى عليه إلى المدعي لشراء اسم الحقل محل النزاع، فالفكرة الأفضل التي تشير إليها العبارة هي في نظر اللجنة عرض مبلغ الشراء عليه بدلا من مطالبته بحذف اسم الحقل. http://www.wipo.org

المطلب الثاني

العوامل المشجعة على السطو الإلكتروني

تتم القرصنة والسطو بقيام شخص طبيعي أو معنوي بتسجيل علامة تجارية لا يمتلكها في صورة اسم حقل على شبكة الإنترنت، بقصد الإضرار بمالكها وبقصد التمهيد لإعادة بيعها بثمن مغالى فيه[1].

ويبيع القرصان أسماء الحقول والعلامات التجارية المشهورة التي سبق له تسجيلها متعمدا التسجيل، وهو مطمئن إلى أن مالك العلامة المشهورة حرصًا منه على سمعة علامته، سوف يسعى لاسترداد هذا الاسم بأي ثمن يطلبه، وسوف نبين فيما يلي أهم الأسباب المشجعة على السطو والقرصنة.

1 - مبدأ الأسبقية في التسجيل:

يسمح مبدأ الأسبقية في التسجيل، والذي يحكم تسجيل أسماء الحقول لأي مشروع أو لأي شخص أن يسجل اسم حقل على شبكة الإنترنت، ما دام أن الاسم لم يسبق تسجيله دون أية شروط أخرى من الجهات المختصة بهذا

---

(1) أمام تزايد قضايا السطو الإلكتروني بأعداد لا سابق لها في سنة 2007، أصبح تطور نظام تسجيل أسماء حقول شبكة الإنترنت يثير مزيدًا من القلق عبر العالم، وشهدت سنة 2007 رقما قياسيا في عدد الشكاوى بشأن حالات السطو الإلكتروني المزعوم، أي التسجيل التعسفي للعلامات التجارية على شبكة الإنترنت، التي أودعت لدى مركز التحكيم والوساطة التابع للمنظمة العالمية للملكية الفكرية (الويبو)، وهو ما يعادل زيادة بنسبة 18٪ على سنة 2006 و48٪ على سنة 2005 في عدد المنازعات بشأن الحقول العليا المكونة من أسماء عامة (gTLD) والمكونة من رموز بلدان (ccTLD). والإحصائيات متوفرة على الموقع التالي:
http://www.wipo.int/pressroom/ar/articles/2008/article_0015.html#table1

التسجيل[1].

والمبدأ المعمول به في هذا المجال أنه مـن يـأتي أولا تـتم خدمتـه أولا First Come First Served , وقد شجع ذلك على ظهور القرصنة والسطو الإلكـتروني عـلى شـبكة الإنترنـت، حيـث استغلت المشروعات هـذا المبـدأ وسـارعت إلى تسـجيل العديـد مـن أسـماء الحقـول التـي تمثـل علامات تجارية مشهورة، فعندما يرغب أصحاب العلامـات المشـهورة في تسـجيل أسـماء حقـول إلكترونية لتمثيل علامتهم يفاجئون بسبق تسجيل هذه العناوين من جانب مشروعات وأشخاص لا يملكون أي حق مشروع عليها، فيقومون بشرائها بأثمان باهظـة، وقـد أدى مبـدأ الأسـبقية ومـا صاحبه من غياب الرقابة عليه إلى زيـادة عمليـات القرصـنة والسـطو الإلكـتروني والاعتـداء عـلى العلامات التجارية.

فمـثلا في عـام 1995 كـان عنـوان الموقـع macdonalds.com المملـوك لشركـة Mc Donald's العالمية الشهيرة المتخصصة في تقديم الوجبات السريعة مسجلا باسم صحفي يعمـل بمجلة Wired الأمريكية, ولقد تمكنت هذه الشركة وبعد مسـاومات ماليـة كبـيرة مـن اسـترجاع هذا العنوان الخاص بها[2].

ويمكن تقسيم معظم النزاعات التي تسببت بها قاعدة من يأتِ أولا يخدم أولا إلى نوعين:

الأول: حين يطالب طرفان أو أكثر بعنوان موقع معين, ويكون لهم الحق في المطالبة به, ومن أمثلة ذلك ما حصل في عام 1994 حين

---

(1) د. شريف محمد غانم، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، مرجع سـابق، ص 101.

(2) د. طوني ميشال عيسى, التنظيم القانوني لشبكة الإنترنت, مرجع سابق, ص77.

سجلت شركة Mark Newton , وهي شركة تقدم أعمال نصح في المعلوماتية, في حين تبين لاحقًا أن كلمة Newton هي في الوقت ذاته ماركة مسجلة لشركة الكمبيوتر العالمية Apple[1].

الثاني: حين تكون الغاية من تسجيل عناوين المواقع الإضرار بحقوق الغير، ومثال ذلك في العام 1994 حين أرادت إحدى الشركات التجارية الأمريكية Kaplan تسجيل عنوان موقع لها في شبكة الإنترنت باسم Kaplan.com ففوجئت بأن عنوان الموقع المذكور سبقتها في حجزه إحدى الشركات المنافسة لها والتي تحمل اسما مختلفا Princton Review[2].

2 - شهرة العلامة التجارية:

ارتبطت شهرة العلامة التجارية بتشجيع الاعتداء عليها وتقليدها عبر شبكة الإنترنت، ويشهد الواقع بذلك، فالعديد من الأحكام الصادرة بإدانة القرصنة صدرت بمناسبة الاعتداء على علامات تجارية عالمية ومعروفة لدى جمهور كبير من المستهلكين، والأمثلة كثيرة.

وقد عرفت محكمة استئناف باريس العلامة المشهورة في حكمها الصادر في 17 يناير 1996 بأنها "العلامة المعروفة لدى عدد كبير من الجمهور وتتمتع بجاذبية لدى جمهور المستهلكين مستقلة عما تمثله من منتجات وخدمات".

ويعد اختيار القرصان العلامة المشهورة لتسجيل اسم الحقل مؤشرًا على سوء نيته وقصده الحصول على مبالغ كبيرة من تسجيل اسم الحقل، ويعتبر القضاء هذا السلوك من جانب القرصان دليلا على ارتكاب جريمة السطو

(1) http://www.law.georgetown.edu/lc/internic/domain1.html

(2) http://www.patents.com

الإلكتروني.

ويستنبط القضاء من ذلك وجود قرينة على علم المسجل بوجود علامة مشهورة تحمل نفس تسمية اسم الحقل، وقد اختارها المسجل بالذات لتحقيق كسب مادي من وراء التسجيل، ومن ثم لا يستطيع مسجل اسم الحقل أن يثبت حسن نيته بعدم علمه بوجود هذه العلامة، فشهرة العلامة تصلح أن تعد قرينة لافتراض سوء نيته.

ومن تطبيقات ذلك الحكم الصادر من محكمة باريس الابتدائية في 1999/10/19، حيث اعتبرت المحكمة أن تسجيل اسم الحقل Celio.com يمثل اعتداءً على العلامة التجارية Celio[1].

3 - نوع المجال الذي يسجل فيه أسماء الحقل:

يزداد السطو الإلكتروني لأسماء الحقول العامة أكثر من الوطنية، فهذه الأسماء العامة تعتبر مجالا خصبًا لجذب الأشخاص والمشروعات، وذلك لأن هذه الأسماء مشهورة ومعروفة أكثر لجمهور المتعاملين مع شبكة الإنترنت، ولهذا السبب تحرص المشروعات التجارية على أن تمتلك أسماء حقول إلكترونية من هذا النوع لمعرفتها الجيدة لدى الجمهور، مما يساعدها على انتشار علامتها وتسويق منتجاتها بصورة أفضل، كما هو الحال بالنسبة لأسماء الحقول العامة، ويضاف إلى ذلك قلة الرقابة على منتج الأسماء الإلكترونية، حيث لا تتطلب الجهات المنوط بها تسجيل هذه الأسماء أية شهادة أو مستند للتسجيل، في حين أن أسماء الحقول الوطنية التابعة للدول تتطلب لصحة تسجيل هذه الأسماء أن يقدم المسجل شهادة تفيد ملكيته للعلامة التي يرغب في تسجيل اسم حقل يمثلها.

(1) http://www.legalis.net/jnetldecisions/marques/tgi_nanterre_srf.htm

المطلب الثالث

صور السطو الإلكتروني

يحتكر صاحب العلامة المسجلة حق استعمالها كرمز لمنتجاته، فله الحق في الاعتراض على تسجيل أو استعمال الغير لعلامة مشابهة متى ترتب على التسجيل أو الاستعمال خلط أو لبس في أذهان الجمهور، كل ما هنالك أن العلامة المسجلة تحظى بحماية مدنية وجنائية من المشرع، وذلك بخلاف العلامات غير المسجلة التي تحظى بحماية مدنية فقط.

وتزداد فرص الاعتداء على العلامات التجارية خصوصًا على شبكة الإنترنت من جانب مسجلي أسماء الحقول، ويستند القضاء في حمايته لهذه العلامات ضد القرصنة وتقليدها على شبكة الإنترنت للقواعد التي يتضمنها قانون العلامات التجارية، ويفرق القضاء في حمايته للعلامات التجارية على شبكة الإنترنت بين العلامات المسجلة قبل تسجيل اسم الحقل، وتلك المسجلة بعد تسجيل هذا الاسم، على النحو التالي:

أولا: قرصنة العلامات التجارية المسجلة سابقًا:

ينص القانون الاتحادي لدولة الإمارات رقم (37) لسنة 1992م في شأن العلامات التجارية في المادة (37) منه على أن:

(يعاقب بالحبس وبالغرامة التي لا تقل عن (5000) خمسة آلاف درهم، أو بإحدى هاتين العقوبتين:

1) كل من زور علامة تجارية تم تسجيلها طبقًا للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور، وكل من استعمل بسوء القصد علامة تجارية مزورة أو مقلدة.

2) كل من استعمل بغير حق علامة تجارية مسجلة مملوكة لغيره.

3) كل من وضع بسوء القصد على منتجاته علامة تجارية مسجلة مملوكة لغيره.

4) كل من باع، أو عرض للبيع أو للتداول، أو حاز بقصد البيع منتجات عليها علامة تجارية مزورة أو مقلدة أو موضوعة بغير حق مع علمه بذلك.

5) كل من عرض تقديم خدمات تحت علامة تجارية مزورة أو مقلدة أو مستعملة بغير حق مع علمه بذلك).

كما عاقب قانون حماية الملكية الفكرية المصري الجديد في المادة (113) منه كل من يزور علامة تجارية تم تسجيلها طبقًا للقانون، أو قلدها بطريقة تدعو إلى تضليل الجمهور، ولم يقتصر التجريم على تزوير أو تقليد العلامة المسجلة، وإنما امتد إلى استعمال العلامة المقلدة أو المزورة ووضعها بسوء قصد على منتجاته، ويشترط القانون لوقوع هذه الجرائم أن تكون هذه العلامة مسجلة، فالقانون يحمي هذه العلامات المسجلة بالطريقة المنصوص عليها قانونًا[1].

ولا يتردد القضاء المقارن في حماية العلامات التجارية المسجلة من الاعتداء عليها من جانب مسجل اسم الحقل، وقد كرس القضاء في هذا الصدد قضاءً ثابتًا لإدانة السطو الإلكتروني.

ويعتبر القضاء أن صاحب اسم الحقل قد اعتدى على حق مالك العلامة المسجلة سابقًا، فيكون له الحق في رفع دعوى التقليد لنقل اسم الحقل أو

(1) على الرغم من أن المادة (113) من قانون الملكية الفكرية المصري لم تذكر لفظ مسجلة بالنسبة للعلامات التي تحدثت عن حمايتها في الفقرات الثانية والثالثة والرابعة منها، إلا أننا نتفق مع ما ذهب إليه أغلب الفقه من ضرورة كون العلامة مسجلة.

إلغائه والحصول على تعويض لجبر ما أصابه من ضرر.

وقد صدرت أحكام عديدة تدين اعتداء مسجل اسم الحقل على علامات تجارية مسجلة سابقًا قبل تسجيل اسم الحقل[1]، ويدين القضاء أيضًا القرصنة إذا وقعت من جانب مسجل اسم الحقل على اسم مقاطعة أو مدينة معينة تم تسجيلها سابقًا[2].

(1) ومن هذه الأحكام، الحكم الصادر في قضية Lafayette،galaries ، فقد اكتشفت هذه الشركة أن هناك اسم حقل وهو: Lafayette،La يتضمن تقليدًا لعلامتها تم تسجيله على شبكة الإنترنت، فرفعت الشركة المالكة دعوى تقليد ضد مسجل اسم الحقل، وقد استندت المحكمة في إدانتها للسطو على العلامة Lafayette، La،Galaries " إلى نص المادة 2/713 من قانون الملكية الفكرية الفرنسي- والتي تجرم كل تزوير أو تقليد أو استعمال علامة من جانب شخص غير مالك لها وبدون إذن من المالك، والأمر نفسه نجده في الحكم الصادر في قضية info.com،France ففي هذه القضية أدانت المحكمة الابتدائية بباريس تصرف أحد الأشخاص الذي سجل العلامة التجارية info،France المملوكة لراديو فرنس France،Radio، وقد اعتبرت المحكمة أن هناك قرصنة وسطوًا على العلامة التجارية من جانب مسجل اسم الحقل، وأمرت المحكمة بنقل العنوان المتنازع عليه إلى شركة France،Radio وتبليغ شركة NSI المختصة بهذا الحكم.

(2) ومن الأحكام الصادرة في هذا المجال، الحكم الصادر في قضية tropes،Saint ، وتتمثل وقائع هذه القضية في أن مقاطعة tropez،Saint أرادت أن تسجل اسمها عبر شبكة الإنترنت من خلال اسم حقل تعرض فيه بيانات ومعلومات عامة عن المقاطعة، وفوجئت المقاطعة بعد ذلك برفض طلبها لسبق اسم حقل باسمها وهو: tropez.com،Saint من جانب شركة Eurovirtuel، فرفعت المقاطعة دعوى التقليد ضد هذه الشركة على أساس سبق ملكيتها للتسمية tropez،Saint. وقد أدانت المحكمة الابتدائية لـ Droguignan في حكمها الصادر في عام 1997 شركة Eurovirtuel على أساس تقليد الاسم والعلامة المملوكين للمقاطعة، واعتبرت المحكمة أن سبق تسجيل الاسم والعلامة يمنح صاحبه حق احتكار استغلاله، مما يستوجب حماية هذا الحق, وقضت محكمة =

ولا يحول دون الحكم بإدانة السطو الإلكتروني أن يختلف المجال الذي تم تسجيل اسم الحقل فيه عن المجال الخاص بالعلامة التجارية، فمالك العلامة له الحق في تسجيلها في كل المجالات، سواء كانت دولية أو وطنية، ولا يمكن التمسك بأنه يمتلك اسمًا في أحد المجالات[1].

= Versailles الابتدائية في 22 أكتوبر 1998 بوقف استخدام اسم الحقل elancourt.com الذي تم تسجيله من جانب أحد الأشخاص ونقله إلى مقاطعة Elacourt التي تعتبر مالكة للتسمية Elancourt bienvence a elancourt مع فرض غرامة تهديدية في حالة التأخير في نقل العنوان إلى المقاطعة.

(1) وتطبيق هذه الفكرة نجده في أحكام قضائية عديدة منها الحكم الصادر من محكمة Bordeaux عام 1996، وتتمثل وقائع هذه القضية في أن شركة Atlantel صاحبة العلامة التجارية بهذا الاسم قامت بتسجيل اسم حقل لها في المجال الجغرافي الفرنسي وهو altantel.fr، وأرادت هذه الشركة أن توسع من نشاطها وانتشارها، فقررت تسجيل اسم حقل جديد في المجال الدولي "com" ليصبح "altante.com"، وفوجئت هذه الشركة بأن هذا الاسم قد تم تسجيله من جانب إحدى الشركات الأخرى، فرفعت شركة Atlantel دعوى قضائية بالتقليد ضد الشركة الأخيرة على أساس أنها اعتدت على علامتها التجارية المسجلة سابقًا قبل تسجيل اسم الحقل، فتمسكت الشركة المدعى عليها بأن الشركة المدعية تمتلك بالفعل اسم حقل في المجال الجغرافي الفرنسي يمثل علامتها، فالعلامة ممثلة على شبكة الإنترنت ولم يتسبب تسجيل العنوان في الحقل com في أية أضرار لها، وقد رفضت المحكمة هذا الدفع مؤكدة أن مالك العلامة المسجلة له الحق في استخدامها عبر شبكة الإنترنت في أكثر من مجال، ولا يجوز حرمانه من تسجيل عنوان له في المجال الدولي بحجة أن له عنوانًا في المجال الجغرافي لإحدى الدول.
والمبدأ نفسه نجده في الحكم الصادر من محكمة باريس الابتدائية عام 1997، ففي هذا الحكم أدانت المحكمة الاعتداء على العلامة التجارية Framatome التي تملكها شركة بالاسم ذاته والتي تمتلك اسم حقل في المجال الجغرافي الفرنسي وهو: Framatome.fr، واعتبرت المحكمة أن قيام شركة Association internatue بتسجيل اسم الحقل Framatome.com يمثل اعتداءً على العلامة التجارية =

ونستطيع أن نحدد أهم المبادئ التي يجب أن يتم الاستناد عليها عند النظر في أي حالة سطو أو قرصنة على حقل من الحقول يمثل علامة تجارية في بيئة التجارة الإلكترونية، وذلك في النقاط التالية:

1 - مخاطر الخلط كشرط ضروري لإدانة السطو الإلكتروني:

يعاقب قانون الملكية الفكرية المصري الجديد في المادة (1/113) منه بالحبس مدة لا تقل عن شهرين، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين كل من زور علامة تجارية تم تسجيلها طبقًا للقانون أو قلدها بطريقة تدعو إلى تضليل الجمهور، ويفرق هذا النص بين جريمتي تزوير وتقليد العلامة التجارية على غرار ما حدث في ظل قانون العلامات التجارية الأصلية بحيث يصعب التفرقة بينهما، أما تقليد العلامة، فهو صنع علامة تجارية مشابهة للعلامة الأصلية في المظهر العام، دون أن يكون هناك نقل تام لها، مما يؤدي إلى احتمال

= لهذه الشركة.

والأمر نفسه نجده في الحكم الصادر من المحكمة الابتدائية لمدينة Nanterre عام 1999، وتتمثل وقائع هذه القضية في قيام شركة W3 systerns inc بتسجيل اسم حقل على شبكة الإنترنت تعرض فيه قائمة لعناوين إلكترونية كثيرة مملوكة لشركة تجارية مشهورة بغرض بيعها، ومن بين هذه الأسماء يوجد اسم sfr.com فطالبت شركة Reditelphone الفرنسية, وصاحبة العلامة SFR التي تمتلكها, الشركة العارضة وأمرت المحكمة بوقف استخدام الاسم ونقله إلى الشركة الأصلية، ولم تلتفت المحكمة إلى قول شركة W3 systems inc من أن شركة SFR لم تتحمل أي ضرر من جراء تسجيل هذا الاسم، لأنها قد سجلت بالفعل اسم حقل تعرض فيه منتجاتها وهو: SFR.fr ورأت المحكمة أنه من حق شركة SFR أن تسجيل اسمًا جديدًا في المجال الدولي، حتى ولو كانت قد سجلت اسمًا جغرافيًا سابقًا.

الخلط بين العلامتين، وبالتالي تضليل الجمهور[1].

والأمر نفسه نجده في قانون الملكية الفكرية الفرنسي، فحسبما تقضي المادة (2/713) من قانون الملكية الفكرية الفرنسي، يشترط في جريمة تزوير أو تقليد العلامة أن يقع التزوير أو التقليد من جانب شخص غير مالك للعلامة التجارية، وبدون إذن المالك، وفي حالة التقليد يجب أن ترد العلامة المقلدة على منتجات وخدمات مماثلة أو مشابهة لتلك التي تمثلها العلامة التجارية الأصلية، بحيث يترتب على ذلك خلط في أذهان الجمهور، ويستنتج من مجموع هذه النصوص أن المشرع بتقريره جريمة تزوير أو تقليد العلامة يحمي المستهلك من مخاطر الخلط الذي يتولد في ذهنه نتيجة التشابه أو التماثل بين المنتجات والخدمات التي تمثلها العلامة التجارية.

ولا يختلف الأمر عن ذلك على شبكة الإنترنت، فأحكام القضاء الصادرة في مجال التنازع بين العلامات التجارية وأسماء الحقول تتطلب للمعاقبة على القرصنة تشابه المنتجات والخدمات التي يمثلها اسم الحقل، ويرفض القضاء هذا التشابه على أساس أنه يؤدي إلى خداع الجمهور في حقيقة اسم الحقل.

ولكي يتوصل القضاء إلى وجود مخاطر في الخلط الذي نتج عن تقليد أو تزوير للعلامة، يفحص القاضي محتوى أو مضمون الموقع الإلكتروني من خلال المنتجات والخدمات التي تعرض عليه، ثم يفحص بعد ذلك المنتجات والخدمات التي تمثلها العلامة والفئة التي تم تسجيل هذه المنتجات فيها، فإذا كان هناك تشابه أو تماثل بين هذه المنتجات والخدمات، ينتهي القاضي إلى وجود مخاطر للخلط نتجت من تقليد اسم الحقل للعلامة

(1) د. محمد حسني عباس، الملكية الصناعية والمحل التجاري، دار النهضة العربية، القاهرة، 2000، ص 335.

التجارية.

وتقدير مدى مطابقة محتوى الموقع الإلكتروني للمنتجات التي تمثلها العلامة التجارية مسألة موضوعية يترك تقديرها لقاضي الموضوع حسب ظروف كل حالة على حدة، ومع ذلك تشير آراء الفقه وأحكام القضاء إلى معايير مختلفة لتقدير التشابه بين المنتجات والخدمات، ومن هذه المعايير المعيار الموضوعي الذي ينظر إلى مدى توافر عناصر قريبة في المنتجات والخدمات المعروضة في القضية، ومن هذه العناصر مدى التقارب بين المنتجات والاستخدام المشترك لها، وتستند بعض أحكام القضاء إلى المعيار الشخصي الذي يركز على اعتقاد المستهلك بأن المنتجات والخدمات المتشابهة تنتمي إلى مصدر واحد، فمنتجات العطور والمجوهرات التي لها اسم واحد تترك الانطباع لدى المستهلك بأن منتجها واحد على أساس أنها أمور مساعدة على التجميل[1].

(1) ومن التطبيقات القضائية التي أدانت اعتداء اسم الحقل على العلامة التجارية استنادًا إلى استنتاج التشابه من فحص مضمون الموقع، الحكم الصادر من محكمة استئناف Versailles في 14 سبتمبر 2000، وأيضًا الحكم الصادر من المحكمة الابتدائية لـ Draguignan في 8 أبريل 1998، وإذا انتهت المحكمة إلى تماثل محتوى اسم الحقل مع فئة المنتجات والخدمات التي تمثلها العلامة التجارية، فإنها لا تتردد في قبول دعوى الاعتداء على العلامة التجارية، ومن تطبيقات ذلك الحكم الصادر من المحكمة الابتدائية لباريس عام 2000، فقد انتهت المحكمة في هذا الحكم إلى أنه بمطابقة محتوى الموقع الإلكتروني للمنتجات التي تمثلها العلامة التجارية يتضح أن استخدام الغير للعنوان الإلكتروني دون إذن مالك العلامة يشكل تقليدًا لهذه العلامة حسبما تقضي المادة 2/713 من قانون الملكية الفكرية الفرنسي، والأمر نفسه نجده في الحكم الصادر في قضية Grosfillex فبعد أن فحصت المحكمة محتوى ومضمون اسم الحقل grosfillex.com الذي تم تسجيله من جانب شركة أخرى، انتهت المحكمة إلى وجود تماثل بين المنتجات والخدمات التي تعرض من =

أما إذا تأكد القاضي بعد فحصه لمحتوى ومضمون اسم الحقل من اختلافات المنتجات والخدمات التي تعرض على العنوان عن تلك التي تمثلها العلامة، فإنه لا يتردد في رفض دعوى التقليد[1].

وقد قضت المحكمة الابتدائية في حكمها الصادر في 14 سبتمبر 2000، ومن بعدها محكمة الاستئناف في حكمها الصادر في 22 مارس 2001، بعدم ثبوت تقليد العلامة التجارية Lotto، وأكدت المحكمة أنه بافتراض أن اسم الحقل Bananalotto.com جاء متضمنًا مصطلح lotto فهذا لا يكفي في حد ذاته لتبرير ادعاء تزوير أو تقليد العلامة lotto وفقًا للمعنى الوارد في المادة 2/713 من قانون الملكية الفكرية الفرنسي، ويجب أن يترتب على التقليد خلط في أذهان الجمهور، وهو أمر لا يتوافر في القضية المنظورة.

والأمر نفسه نجده في الحكم الصادر من محكمة استئناف Versailles بتاريخ 29 مارس 2000 في القضية المعروفة باسم Commune

= خلال الموقع وتلك التي تمثلها العلامة التجارية.

(1) وهذا ما أشارت إليه محكمة Natuerre الابتدائية عام 2000، وتتمثل وقائع هذه القضية في أن الشركة الفرنسية للألعاب رفعت دعوى تقليد ضد شركة Bingonet على أساس أنها قامت بتسجيل اسم الحقل: Bongonet.com وأن هذا الاسم يمثل اعتداءً على العلامة التجارية "Loto" التي تمتلكها شركة Bingonet بدفاعين، يتمثل الأول في أن اسم الحقل المسجل من جانبها لا يمثل اعتداء على العلامة التجارية Loto، حيث إن المصطلح لم يرد كما هو اسم الحقل، وإنما أضيف إليه حرف (T)، كما أنه قد أضيف إليه مصطلح جديد هو Banana، ويكفي هذا التغيير في رأيها لاستبعاد أي تشابه بين المصطلحين، مما يعهد للعنوان التجاري بخصوصية وتميز اتجاه العلامة التجارية، ويتمثل الدفع الثاني في عدم وجود مخاطر للخلط نشأت في ذهن الجمهور بسبب اسم الحقل المذكور، ومن ثم تفتقد دعوى التقليد أهم شروطها.

Elancourt ، فقد ألغت محكمة الاستئناف في هذا الحكم حكم محكمة Versailles الابتدائية الصادر في 22 أكتوبر 1999، والذي انتهى إلى وجود خلط بين الموقع الذي سجله أحد الأشخاص لعرض معلومات خاصة عليه، وبين اسم المقاطعة الذي سجلته في صورة علامة تجارية، ووجدت محكمة الاستئناف أنه بمقارنة محتوى ومضمون اسم الحقل المسجل بالعلامة التجارية، لم يظهر بشكل واضح وجود أية مخاطر للخلط في أذهان الجمهور، بل على العكس يظهر بالنسبة لمستخدمي شبكة الإنترنت أن هذا الاسم الذي تم تسجيله عنوان خاص لا عنوان عام تملكه المقاطعة.

والواقع أن القضاء الفرنسي يستند في تقريره لمدى التماثل والتشابه بين المنتجات والخدمات إلى حكم محكمة العدل الأوروبية الصادر في قضية Canon في 29 سبتمبر 1988، ففي الفقرة 24 من هذا الحكم أكد المجلس أن تقدير التشابه بين المنتجات والخدمات محل الدعوى يجب أن يأخذ في اعتباره كل العوامل وثيقة الصلة بالموضوع، والتي تبين العلاقة بين المنتجات والخدمات، ومن هذه العوامل طبيعة المنتجات والخدمات، طريقة استخدامها، نوعها، خصائصها التنافسية أو التكاملية.

وإذا كان القضاء الفرنسي يفحص مضمون الأنشطة التي يباشرها مسجل اسم الحقل حتى يتوصل إلى وجود خلط أو لبس أم لا، فإن القرارات الصادرة من مركز التحكيم والوساطة التابع للمنظمة العالمية للملكية الفكرية تنتهج نهجًا آخر، فهذه القرارات تركز بالدرجة الأولى على الاسم الذي يتكون منه اسم الحقل وما إذا كان يتضمن العلامة التجارية الأصلية أم لا، فإذا كان اسم الحقل يتضمن العلامة التجارية كعنصر مميز لا يمكن الاستغناء عنه فإنه يعد مماثلا أو مشابهًا للعلامة التجارية بغض النظر عن

الأنشطة التي يباشرها مسجل اسم الحقل والعكس صحيح[1].

2 - العبرة في تقدير التشابه بالمظهر العام لاسم الحقل:

تقدير الخلط الذي يتركه تقليد العلامة يجب أن يستند إلى النظرة العامة للعلامتين الأصلية والمقلدة دون التركيز على الجزئيات الصغيرة التي تتكون منها العلامتان، فجريمة التزوير تقع متى تشابهت العلامتان في النظرة العامة لهما حتى ولو تباينت كل منهما في بعض العناصر المكونة لها، ولهذا مثلا قضت محكمة النقض المصرية بأنه ليس الفصل في التمييز بين علامتين باحتواء العلامة على حروف أو رموز أو صور مما تحتويه العلامة الأخرى، فالعبرة بالصور العامة التي تستقر في الذهن نتيجة تركيب هذه الصور أو الرموز أو بالشكل الذي تبرز به في علامة أخرى، بصرف النظر عن العناصر المركبة فيها، وعما إذا كانت الواحدة فيها تشترك في جزء أو أكثر مما تحتويه الأخرى.

وتقرير وجود تشابه بين علامتين والذي من شأنه أن يخدع جمهور المستهلكين من المسائل الموضوعية التي تدخل في سلطة قاضي الموضوع

(1) ومن تطبيقات هذه الفكرة القرار الصادر في القضية Ataltic cost of America في 26 فبراير 2002، ففي هذه القضية وجدت اللجنة التي نظرت النزاع أن الشركة المدعى عليها Stenven Zahakis قد سجلت اسم الحقل Swerg.com مستخدمة بذلك العلامة التجارية التي تمتلكها الشركة المدعية وهي Swreg وانتهت اللجنة تبعًا لذلك إلى أن اسم الحقل مماثل لهذه العلامة مما يثير الخلط واللبس بينهما، والأمر نفسه نجده في القرار الصادر في 22 مارس في قضية Toyota Fence، ففي هذه القضية انتهت اللجنة الإدارية التي نظرت النزاع إلى أن اسم الحقل Toyota،occaisions.com الذي سجلته شركة brain،Computer مماثل للعلامة التجارية المشهورة Toyota، وبنت اللجنة قرارها على أن هذا الاسم يتكون بصفة أساسية من كلمة Toyota التي تعتبر عنصرًا مميزًا ومستقلا فيه.

بلا معقب عليه من محكمة النقض، متى كانت الأسباب التي أقيم عليها تبرر النتيجة التي انتهى إليها.

وقضي بأن تقليد العلامة التجارية هو اصطناع لعلامة مشابهة فى مجموعها للعلامة الأصلية من شأنها أن تضلل جمهور المستهلكين المخاطبين بالعلامتين لوقوع اللبس بينهما، ويؤخذ فى تقدير التشابه المضلل بين العلامتين التجاريتين وعي وإدراك جمهور المستهلكين العاديين المخاطبين بهما وقدرتهم على التمييز بينهما، والتقليد الذى يؤدي للخلط والتضليل لا يمكن صبه فى قالب واحد، وإنما تخضع كل حالة لظروفها وللصلة والعلاقة بين العلامتين، والمعيار فى تقدير الشبه المضلل هو معيار موضوعي وهو معيار الشخص العادي، وهو ما تستخلص وجوده من عدمه محكمة الموضوع دون معقب عليها من محكمة التمييز متى كان استخلاصها سائغًا وله أصله الثابت فى الأوراق[1].

ويطبق القضاء هذا المبدأ عند نظر دعوى التقليد المتعلقة بأسماء الحقول، فيكفي لثبوت التقليد وجود تشابه في المظهر العام بين العلامة التجارية واسم الحقل دون الالتفات إلى اختلافهم في الجزئيات الصغيرة، فعادة ما يقوم أصحاب أسماء الحقول بتسجيل عناوينهم مع إضافة أو حذف بعض الحروف لاسم الحقل الإلكتروني، بحيث تتميز العلامة التجارية، ويتهرب بذلك من أحكام جريمة التقليد، بيد أن القضاء يقف بالمرصاد لكل هذه التصرفات، ويقضي بالتقليد لمجرد التماثل أو التشابه في المظهر الإجمالي بين العلامة واسم الحقل، ومن أسماء الحقول التي انتهى القضاء إلى أنها تثير الخلط واللبس نجد مثلا اسم الحقل koddak.com الذي

(1) القاعدة الصادرة سنة 2008 حقوق التي تضمنها حكم محكمة التمييز بدبي بتاريخ 24-11-2008 في الطعن رقم 2008 / 227 طعن تجاري.

يختلط بالعلامة المشهورة Kodak، والاسم micro-soft.com الذي يختلط بالعلامة التجارية Microsoft واسم الحقل: la-cost.com الذي يختلط بالعلامة Lacost.

ومن تطبيقات هذه الفكرة ما قضي به من أن الفرق في الجزئيات الصغيرة لا يمنع من وجود تشابه مرئي أو سمعي، ولا يكفي للتهرب من أحكام جريمة التزوير أو التقليد.

والأمر نفسه نجده في قرار التحكيم الصادر من مركز التحكيم والوساطة التابع للمنظمة العالمية للملكية الفكرية "Wipo" عام 2000، ففي هذه القضية تمسك المدعى عليه بأن هناك فارقًا واضحًا بين العلامة التجارية:Dodi Fayed واسم الحقل: dodielfyaed.com، وأن هذا الفارق يكفي لاستبعاد التشابه بين الاثنين، ومن ثم لا تنطبق أحكام التقليد، وقد رفضت هيئة التحكيم التي نظرت الدعوى هذه الحجة، وأكدت أن اسم الحقل: dodielfyed.Com يعتبر مشابهًا للعلامة التجارية Dodi Fayed فلكل منهما نفس المظهر الإجمالي والصورة العامة، ولا يقدح في الأمر إضافة الحرفين el إلى اسم الحقل[1].

وقضي أيضًا بأن العلامة التجارية Lancome قد تم تقليدها من جانب اسم الحقل lankom.com وجاء في هذا الحكم أنه من المؤكد أن استخدام التسمية lankom من جانب شركة grandtotal يعتبر تقليدًا شبه حرفي للعلامة التجارية lancome وإبدال الحرف (k) بالحرف (c) وحذف الحرف (e) لا يستبعد وجود تطابق بينهما، ولا يكفي لاستبعاد التقليد.

وتطبيقًا لذلك أيضًا انتهى مركز التحكيم والوساطة التابع للمنظمة العالمية للملكية الفكرية WIPO في قضية Volve trademark إلى

(1) http://www.wipo.org

النتيجة السابقة نفسها، ففي القرار الصادر في 22 مارس 2002، قرر المركز نقل اسم الحقل volvoinsurance.com إلى شركة Volvo مالكة العلامة التجارية المشهورة بهذا الاسم، وأسست الهيئة الإدارية التي نظرت النزاع قرارها على الخلط واللبس الذي سيتولد لدى العامة عندما يسمعون ويقرءون اسم الحقل محل النزاع، حيث سيعتقدون أنه ملك الشركة مالكة العلامة التجارية المشهورة(1).

كما قضت محكمة استئناف باريس في حكمها الصادر عام 2000 بخطأ تمسك شركة P بأن اسم الحقل الذي سجلته وهو poeme.com لا يعد تقليدًا للعلامة التجارية poeme، وتستند في ذلك إلى اختلاف تسميتها عن التسمية الأخيرة بوجود Accent circonflexe على الحرف (e)، وهذا لا يتواجد في العلامة التجارية المعروفة، وانتهى الحكم إلى أن هذا الدفع غير مقبول استنادًا إلى تشابه التسمية poeme بالعلامة Poeme وأن وضع Accent لا يمنع هذا التشابه ولا يمنع وجود التقليد.

هذا بالإضافة إلى أن إضافة ملحق معين لاسم الحقل مثل:.com أو.org لا يجعله متميزاً عن العلامة التجارية، ولا يستطيع مسجل الاسم أن يتمسك به لانتفاء مسئوليته عن التقليد، ولا يختلف الأمر إذا أدخل مسجل اسم الحقل اسم المنتج في هذا الاسم، فإدراج اسم المنتج لا يحول دن وجود تشابه بين الاسم والعلامة، مما يقوم به التقليد، فأسماء الحقول الإلكترونية: rolex.com وrolex-watches.com وroles-pen.com وroles-man.com و-rolex deisgm.com كلها أسماء مقلدة للعلامة التجارية Rolex.

ومن تطبيقات هذه الفكرة أيضًا ما قضت به المحكمة الابتدائية لباريس

(1) http://www.wipo.org

في 25 مايو 1999 من أن اسم الحقل Glaiaries - lafaytte.com يعد تقليدًا للعلامة التجارية Galaries-lafaytte، وأن إضافة الملحق .com لم يغير في صورة الاسم، ولم يميزه بخصوصية عن العلامة التجارية.

أما إذا كان اسم الحقل قد قلد العلامة التجارية في أحد عناصرها فقط دون باقي العناصر، فإن تقدير وجود التقليد المعاقب عليه أمر يتوقف على أهمية العنصر الذي تم تقليده، فإذا كان من الممكن فصل هذا العنصر، بحيث يصبح مميزًا في حد ذاته، فإن تقليده من جانب اسم الحقل يمكن اعتباره خطأ على أساس دعوى التقليد.

ومن تطبيقات هذه الفكرة أيضًا القرار الصادر من مركز التحكيم والوساطة التابع للـ WIPO في 6 مارس 2002 في قضية Nokia compration، ففي هذه القضية ادعت شركة Nokia أن اسم الحقل Nokiaheaven-uk.com مماثل أو مشابه لعلامتها التجارية، وطالبت اللجنة بنقل هذا الاسم لها، فوافقت اللجنة على طلب الشركة المدعية، ورفضت حجة الشركة المدعى عليها (Nick holoms) بأن الاسم محل النزاع غير مماثل أو مشابه للعلامة المذكورة، وأضيفت إلى كلمة nokis عبارة طويلة وهي heaven-ul.com مما جعله متميزًا عن العلامة الأصلية، فوجود كلمة واحدة وهي Nokia لا تجعله مشابهًا للعلامة الأصلية، وقد أكدت اللجنة في رفضها لهذه الحجة أن كلمة Nokia التي يتضمنها اسم الحقل هي كلمة أساسية في الاسم، وأنه بدونها لا يكون للاسم معنى، ولما حرصت الشركة المدعى عليها على تسجيله من البداية[1].

ونخلص من ذلك إلى أن الأحكام الصادرة في مجال التنازع بين العلامة التجارية وأسماء الحقول تطبق نفس الفكرة التي يطبقها القضاء بالنسبة

(1) http://www.wipo.org

للتنازع بين العلامات التجارية، وتقضي هذه الفكرة بأن الخطأ المقصود في كتابة أسماء الحقول أو الاختلافات في جزئيات هذا الاسم عن العلامة التجارية لا يمنع القضاء من الحكم بوجود تقليد للعلامة بسبب هذا التشابه، ولا يستطيع أصحاب أسماء الحقول أن يتمسكوا بهذا الفارق حتى يتهربوا من أحكام التقليد.

3 - مجرد تسجيل اسم الحقل يمثل قرصنة للعلامة التجارية:

يتطلب تقليد العلامة التجارية أو السطو عليها عبر شبكة الإنترنت أن ينشأ خلط بين اسم الحقل والعلامة التجارية كما أسلفنا، بحيث يترتب على هذا الخلط ضرر لصاحب العلامة التجارية، وتضليل الجمهور، وحتى يتوصل القضاء إلى وجود هذا الخلط، فإنه يقوم بفحص محتوى أو مضمون اسم الحقل وصولا في النهاية إلى وجود مثل هذا الخلط من عدمه، وهذا يتطلب بطبيعة الحال أن يمارس صاحب اسم الحقل نشاطًا تجاريًا على هذا الاسم بعرض منتجات وخدمات تماثل أو تشابه المنتجات والخدمات التي تمثلها العلامة التجارية، ولذا يثار التساؤل عما إذا كان مجرد تسجيل اسم الحقل دون ممارسة أي نشاط عليه يشكل تقليدًا للعلامة التجارية أم لا؟

يستند مسجلو أسماء الحقول على حجج في صالحهم، مفادها أنهم لم يفعلوا شيئًا سوى تسجيل اسم الحقل، وأنهم لم يمارسوا أية أنشطة من خلال هذا الاسم، ومن ثم لا يمكن الادعاء بأن هناك تماثلا أو تشابهًا بين الأنشطة يتولد عنه خلط في أذهان الجمهور، هذا بالإضافة إلى أنهم لم يتسببوا في حدوث أية أضرار لمالكي العلامات التجارية بسبب هذا التسجيل[1].

والواقع أن القضاء يرفض هذه الحجج جملة وتفصيلا، ويعتبره اعتداءً

(1) د. شريف محمد غانم، حماية العلامات التجارية عبر الإنترنت، مرجع سابق، ص134.

على حق مالك العلامة التجارية، ويتمثل في منع مالك العلامة من تسجيل اسم يمثل علامته على شبكة الإنترنت، ولذا فإن تسجيل أسماء الحقول Mercedes.com وMacdonalds.com يشكل تقليدًا وقرصنة للعلامات المشهورة بهذا الاسم، حتى ولو لم تستخدم هذه المواقع لعرض سيارات مرسيدس أو منتجات التغذية التي تقدمها محلات ماكدونالدز.

وتطبيق هذه الفكرة نجده في قضية galleries-Lafayette، فقد ساقت شركة association excellence François الحجج السابقة أمام المحكمة الابتدائية لباريس عام 1999، وقد رفضت المحكمة هذه الحجج وأكدت أن مجرد تسجيل اسم الحقل: galaries-Lafayette يعني أن الشركة المسجلة حجزت لنفسها موقعًا بذات الاسم على شبكة الإنترنت ومنعت الشركة الأصلية من تسجيل هذا الموقع، ويشكل هذا العمل تقليدًا للعلامة الأصلية، والأمر نفسه طبقه القضاء في قضية SFR، ففي هذه القضية اعتبر القضاة أن شركة Radiotelephone قد تحملت ضررًا تمثل في اضطرابات تجارية نتجت من مجرد تسجيل اسم الحقل SFR.com من جانب شركة w3 systemes.inc فالشركة الأصلية مالكة العلامة لم يعد في استطاعتها أن تسجل اسم حقل في المجال الدولي ليمثل علامتها بسبب التسجيل الذي تم من جانب شركة لا تمتلك حقوقًا مشروعة على العلامة التجارية[1].

والأمر نفسه في قضية L'oreal حيث قررت المحكمة أنه "من المؤكد أن حيازة اسم حقل على شبكة الإنترنت يشكل تقليدًا للعلامة التجارية، وتأكد الأمر أيضًا في حكم حديث صدر في قضية بتسجيل اسم الحقل: lankom.com، وقررت المحكمة أن تسجيل هذه الأسماء يشكل تقليدًا لها.

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 415.

كما تستند بعض الأحكام لعبارة "موقع تحت الإنشاء" "Site on constriction" التي يكتبها مسجلو أسماء الحقول الذين لا يستغلونها على صفحة هذه الأسماء، فاعتبر القضاء أن كتابة هذه العبارة نوع من استغلال الموقع، وهذا التفسير نجده في الحكم الصادر من المحكمة الابتدائية لمدينة Lille عام 2000 والمتعلق باسم الحقل Kiloutuou.com، فقد اعتبرت المحكمة أن وضع عبارة موقع تحت الإنشاء التي وضعتها شركة spenser aniakou على هذا العنوان تشكل تقليدًا للعلامة التجارية kiloutou.

ويستند القضاء أيضًا في بعض أحكامه إلى التفسير الموسع لمصطلح استخدام use الذي تنص عليه قواعد تسوية النزاعات المتعلقة بأسماء الحقول "UDRP" التي وضعتها شركة ICANN عام 1999[1]، وتقضي هذه القواعد بنقل اسم الحقل إلى مالك العلامة المسجلة إذا تم

(1) منذ ديسمبر/ كانون الأول 1999، أي تاريخ بدء العمل بالسياسة الموحدة (UDRP) التي تتيح وسيلة سريعة ومعقولة التكلفة لتسوية المنازعات، وحتى ديسمبر/ كانون الأول 2007، أودعت لدى المركز 33412 قضية بناء على السياسة الموحدة أو بالاسترشاد بها (في فئتي gTLD وccTLD)، وقد شملت 30122 اسم حقل مختلف، وفي سنة 2007 وحدها شملت القضايا المرفوعة أمام الوايبو أكثر من 100 طرف مسمًّى في تلك المنازعات، وهي طفرة كبيرة في عدد البلدان الممثلة كأطراف مدعى عليها من 72 في سنة 2000 إلى 96 في سنة 2007، مما قد يدل جزئيا على التوزيع الجغرافي للنفاذ إلى شبكة الإنترنت عبر مختلف الأقاليم والمناطق، وظلت الولايات المتحدة الأمريكية وفرنسا والمملكة المتحدة القواعد الأكثر استعمالا من قبل المدّعين، وكانت كل من الولايات المتحدة الأمريكية والمملكة المتحدة والصين من البلدان الممثلة أكثر كأطراف مدّعى عليها.
http://www.wipo.int/pressroom/ar/articles/2008/article_0015.html#table1

تسجيل اسم الحقل أو استخدامه بسوء نية، وتذهب الهيئات الإدارية التي تنظر النزاعات وفقًا لهذه القواعد إلى أنه يجب تفسير مصطلح "use on bad faith" استعمال بسوء نية بشكل واسع، بحيث يتضمن مجرد تسجيل اسم الحقل حتى في غياب أي نشاط على صفحة الموقع.

وقد طبق مركز التحكيم التابع لمنظمة التجارة العالمية هذا التفسير في الحكم الصادر منه في قضية World wrestling federation inc ففي هذه القضية أكدت هيئة التحكيم أن مجرد عرض اسم الحقل للبيع بعد تسجيله يعد استعمالا بسوء نية، مما تقوم معه جريمة تقليد العلامة التجارية وفقًا للفقرة الثالثة من المادة الرابعة من قواعد UDRP.

كما تكيف بعض الأحكام طبيعة اسم الحقل في حالة سكونه وعدم ممارسة أية أنشطة من خلاله بأنه منتج أو خدمة في حد ذاته تتبع الفئة (38) من فئات المنتجات والخدمات، كما يحددها قانون الملكية الفكرية الفرنسي، وكذلك التصنيف الدولي للعلامات التجارية، ومن المعروف أن هذه الفئة مخصصة للاتصالات التي تتم بين الحاسبات الآلية، ومن ثم حتى يتوصل القاضي إلى وجود تقليد أم لا من مجرد تسجيل اسم الحقل عليه أن يتأكد من وجود تسجيل سابق للعلامة التجارية في هذه الفئة، فإذا كانت العلامة محل النزاع مسجلة في هذه الفئة، فإن تسجيل اسم الحقل بعد ذلك يعني تقليدًا للمنتجات والخدمات التي تدخل في الفئة (38)، ومن ثم يكون من حق مالك العلامة حمايتها عن طريق دعوى التقليد.

وفي الفرض العكسي الذي لا تكون فيه العلامة مسجلة في الفئة (38)، فإن مجرد تسجيل اسم الحقل دون ممارسة أي نشاط عليه لا يعد اعتداءً عليه لأنه يمثل منتجًا أو خدمة تسجل في هذه الفئة بعيدًا عن الفئة المسجل فيها المنتجات التي تمثلها العلامة.

ويترتب على ذلك أن القضاة يفرقون في طبيعة اسم الحقل بحسب ما إذا كانت تمارس عليه أنشطة أم لا من جانب صاحبه، وذلك بهدف إدانة أي اعتداء على العلامة التجارية وحمايتها بشكل مستقل عن المنتجات والخدمات التي تعرض على اسم الحقل، فإذا كان اسم الحقل مستغلا فإن القضاء يعتبر العنوان مجرد وسيلة للإعلان عن المنتجات، أو مجرد عنوان للمشروع على شبكة الإنترنت، ومن ثم يكون التعويل على نوعية المنتجات أو الخدمات يشابه خدمة الاتصالات التي تسجل في الفئة (38)، وبمعنى آخر تتحول طبيعة الاسم من مجرد وسيلة إلى منتج أو خدمة[1].

ومن الأحكام القضائية التي تبنت هذه المغايرة في طبيعة اسم الحقل، الحكم الصادر في قضية ;Atlantal السابقة، ففي هذه القضية حددت المحكمة الفئة التي من الممكن أن يندرج فيها اسم الحقل بأنها الفئة (38)، والخاصة بخدمات الاتصالات, ومن ثم انتهت المحكمة إلى وجود تقليد على أساس أن العلامة التي يملكها المدعي تمثل منتجات تنتمي إلى هذه الفئة، ومن ذلك أيضًا الحكم الصادر في قضية st-tones، حيث رفضت المحكمة دفع المدعى عليها وهي شركة Eurovirtuel بأنها لم تمارس أية أنشطة من خلال اسم الحقل Saint-tropes.com وأشارت المحكمة إلى خدمة الاتصالات التي ينتمي إليها اسم الحقل، حتى ولو اقتصر الأمر على مجرد تسجيله، وفي قضية اسم الحقل SFR.com على شبكة الإنترنت يشكل تقليدًا للعلامة التجارية SFR، هذا التقليد يمكن استنتاجه من واقعة التسجيل ذاتها.

نخلص من ذلك إلى أنه حرصًا من القضاء على توفير أكبر حماية ممكنة للعلامات التجارية على شبكة الإنترنت فإنه يعاقب على كل صور

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 432.

الاعتداء عليها، حتى ولو اقتصر الاعتداء على مجرد تسجيل اسم الحقل، ويبدو أن القضاء الصادر في مجال منازعات أسماء الحقول قد تأثر بالقضاء السابق الصادر بخصوص العلامات التجارية، فقد اعتبر هذا الأخير أنه من الممكن أن يستنتج التقليد من عمل مادي يتمثل في مجرد إيداع طلب تسجيل العلامة اللاحقة، حتى ولو لم يكن هناك استخدام لهذه العلامة.

ثانيًا: قرصنة العلامات التجارية المسجلة لاحقًا:

على خلاف الفرض السابق في هذا الفرض تكون العلامة التجارية لاحقة في تسجيلها لاسم الحقل، ففي هذا الفرض يعتبر القضاء أن اسم الحقل يشكل عنصرًا من عناصر الملكية المعنوية للمشروع يحميه القانون من أي اعتداء عليه، وكأنه علامة تجارية يجب حمايتها إذا كانت سابقة لعلامة أخرى، فيعول القضاء على أسبقية اسم الحقل للعلامة اللاحقة لكي يرفض الدفع بوجود تقليد هذه العلامة، ويقر بأحقية مسجل اسم الحقل على هذا الاسم، ويعتبر القضاء أن تسجيل العلامة بعد استعمال اسم الحقل يشكل اعتداءً على حق هذا المسجل.

وتطبيق هذا الفرض نجده في الحكم الصادر من محكمة MANS الابتدائية الصادر في 29 يونيه 1999، وتتمثل وقائع هذه القضية في أن شركة SFDI قامت في منتصف يوليو عام 1996 باستخدام العلامة Oceant على شبكة الإنترنت وفقًا لنظام IP، وهو النظام السابق على وجود أسماء الحقول.

وفي 31 يوليو 1996 قامت شركة Mircrovaz بتسجيل العلامة التجارية Oceant لدى مكتب تسجيل العلامات الفرنسي، ثم قامت في 2 سبتمبر 1996 بتسجيل العلامة التجارية لدى نفس المكتب، وقد أرادت هذه الشركة أن تسجل اسم الحقل Oceant.com، ولكنها فوجئت برفض طلبها

لسبق تسجيل هذا العنوان من جانب شركة SFDI منذ أن كان في صورة العنوان الرقمي: IP، فرفعت شركة Mircrovaz دعوى تقليد ضد شركة SFDI على أساس أنها اعتدت على علامتها التجارية بتسجيلها اسم الحقل.

ففي هذه القضية كان النزاع بين اسم حقل سجلته شركة وبين علامة تجارية مملوكة لشركة أخرى تم تسجيلها بعد تسجيل اسم الحقل، وكان التساؤل الذي يفرض نفسه أمام المحكمة: أي من الشارتين يمكن أن يعلو على الآخر، هل اسم الحقل المسجل سابقًا أم العلامة التجارية المسجلة لاحقًا.

هذا التساؤل له أهمية كبيرة في رأي بعض الفقه، على أساس أن المحكمة التي تفصل في الدعوى لابد أن تستند في حكمها إلى نصوص قانون معين، وفي هذا الصدد ستكون نصوص قانون الملكية الفكرية والخاصة بالعلامات التجارية هي أقرب النصوص إلى ذهن القضاء، خاصة في غياب نصوص خاصة تحكم أسماء الحقول، وتنظم نصوص هذا القانون بين أحكامها العلامات التجارية، ولم ترد بها أية إشارة إلى هذه الأسماء، وكان من المنطقي في ظل هذا الوضع أن يكون الحكم الصادر من المحكمة في صالح مالك العلامة الأصلية، بيد أن الحكم قضى بغير ذلك، فالمحكمة اعتبرت أن اسم الحقل واحد من عناصر الملكية الصناعية مثله في ذلك مثل العلامات التجارية، واعتبرت المحكمة أن النزاع في الحقيقة هو نزاع بين علامتين تسبق إحداهما الأخرى في التسجيل، ومن ثم يجب حماية العلامة الأسبق في التسجيل، ولهذا رفضت المحكمة الطلبات المقدمة من الشركة المدعية خاصة المتعلقة بتقليد العلامة، وأكدت المحكمة أن تسجيل العلامة Oceant من جانب شركة Microvaz في 31 يوليو 1996 يشكل اعتداءً على حق مسجل اسم الحقل السابق.

وفي قضية أخرى جمعت بين شركتين أمريكيتين تدعيان حقوقًا على التسمية Moveibuff قامت إحداهما بتسجيل هذه التسمية في صورة اسم الحقل: Moviebuuff.com في عام 1996 قبل تسجيل الأخرى لها كعلامة تجارية في عام 1998، وقد صدر الحكم في هذه القضية لصالح مسجل اسم الحقل استنادًا إلى أسبقية تاريخ تسجيله على تاريخ تسجيل العلامة التجارية، وهذه الأسبقية أدت إلى رفض دعوى التقليد التي حركتها الشركة مالكة العلامة اللاحقة في التسجيل[1].

والأمر نفسه نجده في الحكم الصادر في قضية agaphone عام 1998، فقد رفضت المحكمة في هذا الحكم دعوى تقليد العلامة agaphone من الشركة المالكة لها، على أساس أن تسجيل هذه العلامة إنما حدث بعد تسجيل اسم الحقل agaphone.com بحوالي ستة أشهر، ومن ثم انتهت المحكمة إلى أن الشركة المدعية لم يكن لها أي حق مشروع على العلامة التي تم تسجيلها، ومن ثم لا وجه للحديث عن وجود اعتداء عليها من جانب مسجل اسم الحقل.

وفي حكم صادر من محكمة استئناف باريس عام 2000، أشارت المحكمة إلى مسألة أسبقية تسجيل اسم الحقل، وإلى الأهمية الكبيرة التي تحتلها هذه الأسبقية في تحديد حقوق صاحب اسم الحقل المسجل قبل العلامة التجارية، والمحكمة حرصت على التأكيد على أنه أخذًا في الاعتبار الأهمية الاقتصادية لاسم الحقل بالنسبة للمشروعات التجارية، فيجب على الأطراف أن يثبتوا حقوقهم على هذا الاسم، وبصفة خاصة أن يثبتوا أسبقية تسجيل هذا الاسم على العلامات التجارية المتنازعة معه، وأن يثبتوا أيضًا مخاطر

(1) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 426.

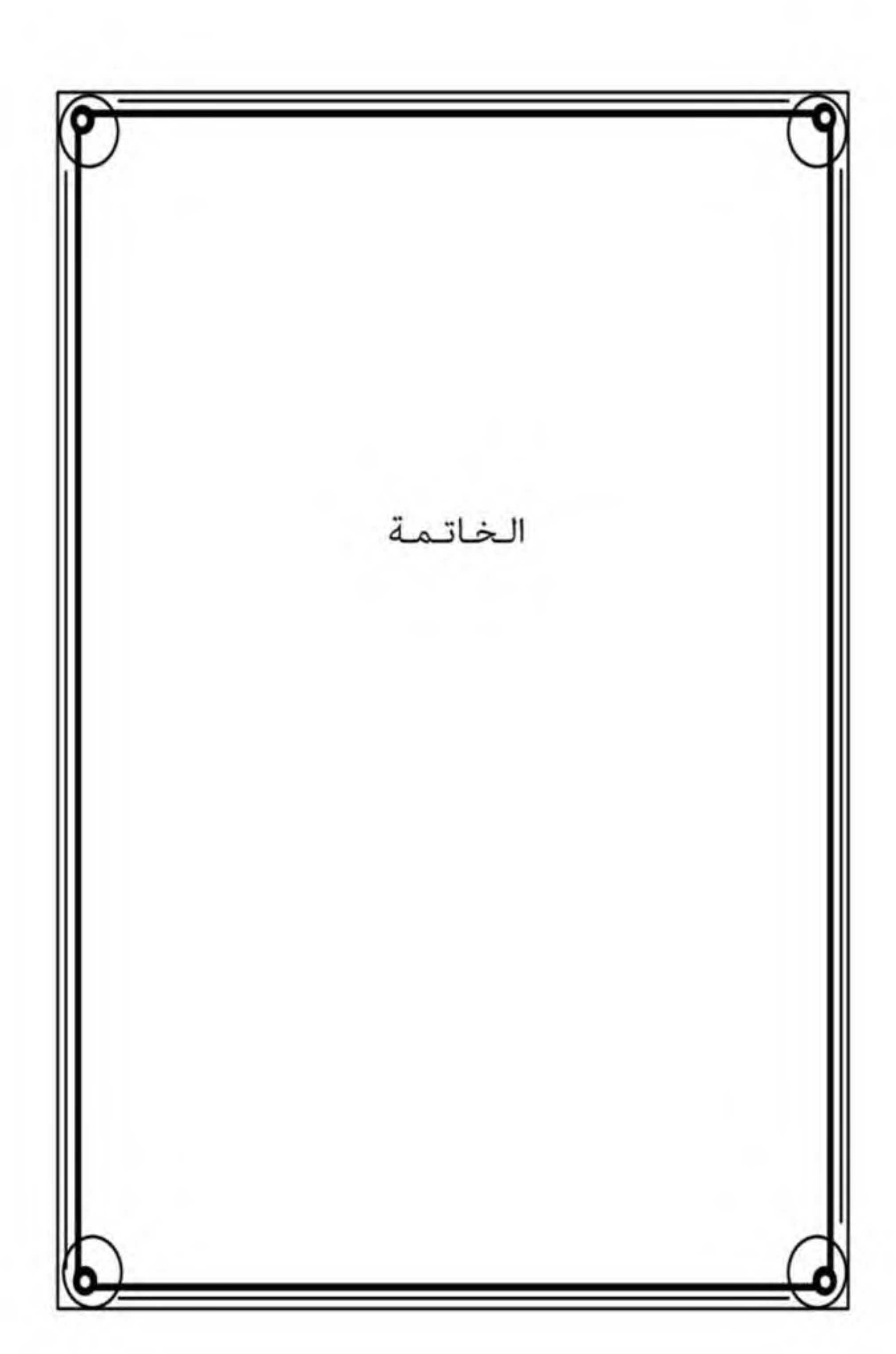
الخلط في أذهان الجمهور التي تنشأ نتيجة الاعتداء على أسماء الحقول[1].

فخلاصة القول أنه على خلاف الفرض الذي تسبق فيه العلامات اسم الحقل في التسجيل، يرفض القضاء دعوى التقليد في الفرض الذي تسجل فيه العلامة التجارية بتاريخ لاحق لتسجيل اسم الحقل[2]، فحق مسجل اسم الحقل يجب أن يحمى أيضًا ما دام أنه لا يمثل اعتداءً على حقوق مالكي العلامات التجارية، ففي مثل هذا الفرض يكيف القضاء اسم الحقل بأنه علامة تجارية يجب حماية حق صاحبها على غرار الحماية التي يتمتع بها مالك العلامة التجارية.



(1) cour d appel de paris.18octobree 2000

(2) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، مرجع سابق، ص 429.



الخاتمة

الخاتمة

ملخص الرسالة - النتائج - التوصيات

أولا: ملخص الرسالة

تناولنا موضوع البحث والذي يدور حول الحماية الجنائية للتجارة الإلكترونية في فصل تمهيدي وبابين، خصصنا الفصل التمهيدي لبحث التنظيم القانوني للإنترنت، وقسمناه إلى مبحثين: الأول لإيضاح ماهية شبكة الإنترنت (المفهوم، النشأة، الأقسام، الخصائص)، وقسمناه إلى أربعة مطالب، تناولنا في المطلب الأول ماهية شبكة الإنترنت ونشأتها وتطورها، وتعرضنا في الثاني لتعريف شبكة الإنترنت باعتبارها وسيلة تواصلية بين الشبكات دون اعتبار للحدود الدولية، وبينا عناصر التعريف، وفي الثالث تناولنا أقسام شبكة الإنترنت الثلاثة (شبكة المعلومات الدولية - البريد الإلكتروني - الاتصال المباشر)، وأوردنا في الرابع خصائص شبكة الإنترنت.

وفي المبحث الثاني تناولنا دراسة قانون الإنترنت من خلال أربعة مطالب: الأول تعريف قانون الإنترنت، والثاني بينا فيه مدارس قانون الإنترنت، وأوضحنا في الثالث خصائص قانون الإنترنت ومراتبه، وبينا في الرابع أقسام قانون الإنترنت.

وتحت عنوان "أساسيات التجارة الإلكترونية وحمايتها" انتقلنا للباب الأول من الدراسة، وقد تناولنا فيه ومن خلال ثلاثة فصول: أساسيات التجارة الإلكترونية، والحماية القانونية للتجارة الإلكترونية، وفي النهاية تجارب التنظيم القانوني للتجارة الإلكترونية.

وقد قسمنا الفصل الأول إلى مبحثين، تناولنا في الأول ماهية التجارة،

وضـمناه أربـع مطالـب تناولنـا فيهـا نشـأة التجـارة الإلكترونيـة وتعريفهـا وأشـكالها وتقـديرها، وخصصنا المبحث الثاني لبيـان خصائــص التجـارة الإلكترونيـة ومعــوقاتها ومسـتقبلها، فقسـمناه لثلاثة مطالب تناولنا فيها خصائـص التجارة الإلكترونية، ومعـوقاتها، ومستقبلها.

وفي الفصل الثاني درسنا، صور مختلفة لحماية التجارة الالكترونية مبتدئين في المبحـث الأول ببيـان المصـلحة المحميـة في التجـارة الإلكترونيـة، وجودهـا وأوجههـا، وتعرضـنا لحمايـة المواقـع الإلكترونية للتاجر، وبحثنا حماية المستهلك الإلكتروني، وأخيراً حماية وسائل الدفع الإلكتروني.

وفي المبحث الثاني تناولنا صور الحماية غير الجنائية للتجارة الإلكترونية، وقسـمناه إلى أربعـة مطالب: الأول الحماية التقنية للتجارة الإلكترونية، والثاني في الحماية المدنية للتجارة الإلكترونيـة، والثالث الحماية الاقتصادية للتجارة الإلكترونية.

وتناولنا في الفصل الثالث تجارب التنظيم القـانوني للتجـارة الإلكترونيـة، وقسـمناه إلى ثلاثـة مباحث: المبحث الأول التجارة الإلكترونية في المـنظمات الدوليـة والإقليميـة، فدرسـناها في لجنـة الأمم المتحدة لقانون التجارة الدولية، وفي قـانون الأونيسـترال - قـانون التوقيعـات الإلكترونيـة - مشروع اتفاقية دوليـة لتنظيـم العقـد الإلكـتروني، ثـم في منظمـة التجـارة العالميـة، وفي المنظمـة العالميـة للملكيـة الفكريـة، وفي منظمـة التعـاون الاقتصـادي والتنميـة (الأنكتـاد)، وفي الاتحـاد الأوروبي، وفي المؤسسات الإقليمية متعددة الأطـراف (اللجنـة الاقتصـادية لأوروبـا التابعـة للأمـم المتحدة - منظمة الأسماء والأرقام الأيكان - ومنظمة التعاون الاقتصادي لآسيا والمحـيط الهـادي - غرفة التجارة الدولية - دور الجامعة العربية).

وفي المبحث الثاني درسنا حماية التجارة الإلكترونية لدى أصحاب

الشراكة في المجتمع المعلوماتي وجور قمة العلومات العالمية في تنظيم التجارة الالكترونية وتناولنا مدلول أصحاب الشراكة، إعلان جنيف 2003، إعلان تونس 2005، وأخيراً أهمية الدور الذي يقوم به المجتمع المدني العلمي في بناء مفاهيم التجارة الإلكترونية.

وفي المبحث الثالث درسنا التجارة الإلكترونية في التشريعات الوطنية، فتناولناها في التشريع الأمريكي وفي التشريعات الأوروبية، وفي كل من كندا واليابان والهند وماليزيا، وأخيراً في التشريعات العربية.

وقد خصصنا الباب الثاني لدراسة الجرائم الواقعة على التجارة الإلكترونية، وقسمناه إلى أربعة فصول: الفصل الأول حول الجرائم الواقعة على المواقع الإلكترونية، تناولنا في المبحث الأول جريمة الدخول والبقاء غير المشروع على مواقع التجارة الإلكترونية (الاختراق - البقاء - أركان الجريمة - المنع من الوصول للمواقع - الاعتراض غير القانوني - موقف التشريعات) وفي المبحث الثاني جريمة إتلاف وتدمير المواقع الإلكترونية فتناولنا صور الإتلاف والتدمير والإتلاف المعنوي وأركان الجريمة والفيروسات وموقف التشريعات، وفي المبحث الثالث تناولنا جريمة التزوير المعلوماتي (ماهية الجريمة وأركانها وصورها وموقف التشريعات) وفي المبحث الأخير بحثنا جريمة الاحتيال الإلكتروني أو الغش المعلوماتي فدرسنا ماهية الجريمة وأركانها وصورها (الاحتيال على النظام - تسليم المال - موقف التشريعات).

ودرسنا في الفصل الثاني الجرائم الواقعة على البيانات، فتناولنا جريمة التعامل بالبيانات بدون ترخيص، وجريمة انتهاك سرية وخصوصية البيانات، وجريمة التصريح ببيانات غير صحيحة، وجريمة التلاعب في بيانات نظم المعلومات، وأخيرًا الاعتداء على نطاق أسماء الدومين.

ثم بحثنا في الفصل الثالث الجرائم الواقعة على وسائل التجارة الإلكترونية ففي المبحث الأول تناولنا الاعتداء على التوقيع الإلكتروني وفي المبحث الثاني جرائم إساءة استخدام بطاقات الدفع الإلكتروني وفي المبحث الثالث: الجرائم الماسة بشهادات المصادقة الإلكترونية.

كما تناولنا في الفصل الرابع والأخير الجرائم الواقعة على الملكية الفكرية والحقوق المجاورة، ففي المبحث الأول بحثنا الحماية الجنائية للمصنف الرقمي، وفي المبحث الثاني، الحماية الجنائية الدولية والوطنية لحقوق مؤلف برامج الحاسب الآلي، وأخيراً وفي المبحث الثالث درسنا تقليد العلامات التجارية.

ثانيًا: النتائج

من خلال البحث وبعد الانتهاء من الدراسة تبينت لنا النتائج الآتية:

1) إن توفير حماية جنائية لأطراف التجارة الإلكترونية - هو بوابة أولى لتحقيق حماية جنائية متكاملة لهذه التجارة، على اعتبار حاجة هذه التجارة إلى ثقة المتعاملين بها، سواء أكانوا تجارًا أم مستهلكين - لا يتأتى ذلك إلا باتخاذ نصوص جنائية تكفل الحماية اللازمة للتجارة الإلكترونية.

2) اهتمام المجتمع الدولي عبر المنظمات الدولية بالتجارة الإلكترونية أسفر عن صدور القانون النموذجي للأمم المتحدة الأونسيترال، والذي وضع قواعد عالمية بإمكان الدول الاسترشاد بها حين تنظيم قواعد التجارة الإلكترونية في قوانينها الداخلية.

3) اهتمام المنظمات الإقليمية بالتجارة الإلكترونية، ومحاولة وضع قواعد لتنظيمها، مثل غرفة التجارة الدولية، والمنظمة العالمية للملكية الفكرية، ومنظمة التعاون والتنمية في المجال الاقتصادي، والاتحاد

الأوروبي من خلال توجيهاته المتميزة في هذا المجال.

4) اهتمــت القــوانين المقارنــة بــدورها أيضًــا بتنظــيم التجــارة الإلكترونيــة، نظــرًا للتطــور التكنولــوجي السرــيع في هــذا المجــال والــذي يجــب أن يواكبــه تطــور تشرــيعي، وضرورة الاهتمام بحماية مواقع هذه التجارة الإلكترونية وأنظمتها ووسائلها من أي اعتداء عليهــا، ومن أمثلة هذه القوانين القانون الأمريكي والقانون الفرنسي.

5) وكما كان ذلك الاهتمام بالتجــارة الإلكترونيــة فقــد كــان هنــاك اهــتمام مــوازٍ مــن الــدول بالجريمة المعلوماتية، فظهرت قوانين مقارنــة تتصــدى لهــذه الجريمــة، كالقــانون الأمــريكي والقانون الفرنسي، كما كان للمنظمات دور كبير، وبالأخص الاتحاد الأوروبي عنــدما أصــدر الاتفاقية الأوروبية للجريمة الافتراضية (اتفاقية بودابست) والتي كانــت نبراسًــا لكثــير مــن الدول في سن تشريعاتها لمواجهة الجرائم الناشئة عن المعلوماتية والثورة التكنولوجية.

6) رأينا أن الدول العربية بدأت تشعر بالخطر من ظاهرة الإجرام المعلوماتي، وضرورة تنظيم التجارة الإلكترونية، وإعطاء التوقيع الإلكتروني والمحررات الإلكترونية الحجيــة في الإثبــات، فصــدر القــانون التونسيــ للمبــادلات والتجــارة الإلكترونيــة، وقــانون إمــارة دبي الخــاص بالمعاملات والتجارة الإلكترونية، وقانون التجارة الإلكترونية البحريني، وقــانون المعــاملات والتجارة الإلكترونية الإماراتي، كما شهدت الســاحة العربيــة إصــدار بعــض الــدول لقــوانين تكافح الجريمة المعلوماتية، حيث كان هناك القــانون العــربي النمــوذجي لمكافحــة جــرائم تقنية المعلومات، وأصدرت دولة الإمارات العربية المتحدة قانونًا اتحاديًا لهذا الغرض، كما أصدرت المملكة العربية السعودية نظامًا

يواجه الجريمة الإلكترونية، بالإضافة إلى إجراء بعض الدول العربية تعديلات على قانون العقوبات للتصدي لمثل هذا النوع من الإجرام، وتوجد مشروعات قوانين لـدى بعـض الـدول الأخـرى، كـما توجد مشروعات قوانين عربية استرشادية على مستوى جامعة الـدول العربيـة، كالقـانون العـربي الاسترشـادي للمعـاملات والتجـارة الإلكترونيـة، والقـانون العـربي الاسترشـادي للإثبـات بالوسـائل الحديثة، بالإضافة إلى مشروع اتفاقية عربية لمكافحة جرائم تقنية المعلومات، وعلى مستوى دول الخليج العربية يوجد مشروع قانون خليجي موحد لمكافحة جرائم المعلومات.

7) تبين لنا وجود قصور في القانون الاتحادي رقم 2006/2، والخـاص بمكافحـة جـرائم تقنيـة المعلومات، الذي لم يتضمن بعض الجرائم الناشئة عن استخدام التقنيات الحديثـة، ومنهـا على سبيل المثـال جريمـة البقـاء غـير المشروع في النظـام المعلومـاتي والمؤثمـة في القـانون الفرنسي، وجريمة سرقة المعلومات، وجريمة النصب المعلوماتي الذي يختلـف عـن النصـب التقليدي، بالإضافة إلى عدم تجريمه الاعتداء غير المشروع على بطاقات الائتمان سـواء مـن صاحب البطاقة أو من الغير، كما أن العقوبات الواردة في القانون تعد عقوبـات تقليديـة، ولم يأت القانون بعقوبات مستحدثة تتلاءم والطبيعة المعلوماتية للجريمة والمجرم.

8) كما يوجد قصور آخر في القـانون الاتحـادي رقـم 2006/1، والخـاص بالمعـاملات والتجـارة الإلكترونية، حيث جاء خاليًا من بعـض المسـائل المهمـة، ومـن أمثلتهـا حمايـة المسـتهلك الإلكتروني، وتنظيم عملية الدفع الإلكتروني، وحمايـة البيانـات الشخصـية، وتنظـيم أسـماء الدومين

وحمايتها، وعدم تنظيمه للتعامل في البيانات الإلكترونية وتجريم التعامل فيها بدون ترخيص.

9) اهتمت أغلب تشريعات الدول المقارنة بالمستهلك الإلكتروني وتوفير أقصى درجات الحماية له، باعتباره الطرف الضعيف في عملية التجارة الإلكترونية، ونشير هنا إلى موقف قانون المبادلات والتجارة الإلكترونية التونسي والذي أورد حماية خاصة للمستهلك الإلكتروني.

10) لحماية الملكية الفكرية المتصلة بالتجارة الإلكترونية دور كبير في استقرار هذه التجارة وحمايتها جنائيًا، وتمثل ذلك في حماية حق المؤلف، وحماية العلامات التجارية، من الاعتداء بكافة أشكاله من قبل الغير، واهتمت القوانين المقارنة بتوفير الحماية اللازمة لها.

ثالثًا: التوصيات

1) **التوصية الأولى**: دعوة المشرع الإماراتي إلى ضرورة توفير مزيد من الحماية الجنائية للتجارة الإلكترونية من خلال المراجعة المستمرة للتشريعات والأنظمة القانونية القائمة لتواكب التطور المستمر في التكنولوجيا.

2) **التوصية الثانية**: إعادة النظر في قانون المعاملات والتجارة الإلكترونية رقم (1) لسنة 2006، وتضمينه حماية المستهلك الإلكتروني، وتنظيم عملية الدفع الإلكتروني، وحماية البيانات الشخصية، وتنظيم أسماء الدومين وحمايتها، وتنظيم التعامل في البيانات الإلكترونية وتجريم التعامل في هذه البيانات بدون ترخيص، وضرورة العمل على سرعة إصدار اللائحة التنفيذية لقانون المعاملات والتجارة الإلكترونية، وتحديد الهيئة الوطنية المختصة بتنظيم جهات التوثيق الإلكتروني وشهادات المصادقة الإلكترونية،

واستخدام أنظمة الدفع الإلكتروني، والعمل على تذليل عقبات هـذا الاسـتخدام، وتطـوير وسـائل الدفع الإلكتروني، والتأكيد على أمـن وسـلامة هـذه الأنظمـة الحديثـة للمـدفوعات الإلكترونيـة لزيادة الثقة لدى المستهلكين والتجار.

3) **التوصية الثالثة**: إعادة النظر أيضًا في قـانون مكافحـة جـرائم تقنيـة المعلومـات رقـم (2) لسنة 2006، والنص على الجرائم التي لم يشملها هذا القانون، كجريمة البقاء غير المشـروع في النظـام المعلومـاتي والمؤثمـة في القـانون الفرنسيـ، وجريمـة سرقـة المعلومـات، وجريمـة النصـب المعلومـاتي والـذي يختلـف عـن النصـب التقليـدي، بالإضـافة إلى ضرورة تجـريم الاعتداء غير المشروع على بطاقات الائتمان سواء من صاحب البطاقـة أم مـن الغـير، كـما نرى ضرورة إدخال عقوبات حديثـة وتـدابير بخـلاف تلـك التقليديـة الـواردة في القـانون، كالإيواء في مأوى علاجي من الإدمان على الاختراق، والحرمان من استخدام التقنيـة لفـترة مـن الـزمن، وخدمـة المجتمـع، وغيرهـا مـن العقوبـات التـي تـتلاءم وطبيعـة الجريمـة المعلوماتية والمجرم المعلوماتي.

4) **التوصية الرابعة:** ضرورة تعديل قانون الإجراءات الجزائية بمـا يتناسـب وطبيعـة الجريمـة المعلوماتية، من ضبط وتفتيش وتحقيـق في هـذه الجـرائم، وكيفيـة التعامـل مـع الـدليل الإلكتروني، وبيان طريقة التعامل مع المجرم المعلوماتي، والاعتداد بالمخرجـات المعلوماتيـة والتوقيـع الإلكـتروني مـع إعطـاء أهميــة خاصــة لــبعض المســائل المتعلقــة بالتجــارة الإلكترونية، مثل سرية البيانات والخصوصية، وكـل هذه المسائل تصـب بغيــر شــك في تقويـة النظـام القانوني للتجـارة الإلكترونية.

5) **التوصية الخامسة:** العمل على إيجاد طرق بديلة للتقاضي في مجال التجارة الإلكترونية تمتاز بالسرعة والخصوصية اللتين تميزان التجارة من جهة والتقنية من جهة أخرى، وتذليل الصعوبات المتعلقة بتسوية المنازعات الناشئة عن التجارة الإلكترونية، ووجوب أن يتم تسويتها بالعديد من أساليب فض المنازعات التي قامت بتأسيسها المنظمات الدولية والمؤسسات الخاصة، نذكر منها: نظام التسوية الإدارية لمنازعات أسماء النطاق، وتسوية المنازعات بالوسائل البديلة، وتسوية النزاع عن طريق نظام التحكيم الإلكتروني، وهي أهم وسيلة لتسوية نزاعات التجارة الإلكترونية لتيسيره الاتصالات بين الأطراف المعنية وتقصير فترة إجراءات التقاضي، وسهولتها وتكلفتها المنخفضة.

6) **التوصية السادسة:** دعوة كافة الدول العربية لوضع تشريعات في مجال التجارة الإلكترونية، وأن تكون هناك معاهدة عربية منظمة لهذه التجارة، خصوصًا وأنها ذات طابع دولي، وعدم الاكتفاء بالتوسع في تفسير النصوص الموجودة أصلا كي تشمل التجارة الإلكترونية، فهذه التجارة لابد وأن تمارس في إطار بيئة قانونية معينة تتفق ومتطلباتها، والاهتمام بالمستهلك الإلكتروني، وإفراد حماية خاصة له، والعمل أيضًا على تطوير التشريعات المتعلقة بالملكية الفكرية، حتى تتلاءم والبيئة الرقمية للتجارة الإلكترونية، واستيعاب الصور الحديثة التي ظهرت للملكية الفكرية وما يتصل بها، وضرورة العمل على تطوير القوانين الأخرى القائمة حتى تتناسب مع التجارة الإلكترونية، كقانون الإثبات.

7) **التوصية السابعة:** دعوة الدول العربية التي لديها فراغ تشريعي إلى

إصدار تشريع خاص بالجرائم المعلوماتية يشتمل علـى جرائم شبكة الإنترنت بشـقيها الموضـوعي والإجرائي، وإنشاء وحدة تحقيقات خاصة تتولى مهمـة التحقيـق في الجـرائم المعلوماتيــة، ومنهـا الجرائم المتعلقة بشبكة الإنترنت والادعاء فيها، وإيجاد وكـلاء نيابـة قضـاة متخصصـين ومـدربين للنظر في الجرائم المعلوماتية وإثباتها والتحقيق فيها نظرًا لحاجتها إلى مهارات خاصة لا تتوافر في القضاء العام، وتعزيز وتنشيط تبادل المعلومات بين الأجهزة الأمنيـة والقضـائية مـن جهـة، وبـين خبراء نظم المعلومـات من جهة أخرى، لمعرفة أبعاد الجرائم المعلوماتية، ومقدار الأضرار الناشـئة عنها، وسمات مجرميها، وأساليب منعها وملاحقة مرتكبيها.

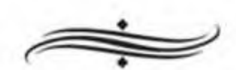
8) **التوصية الثامنة:** بالإضافة إلى ضرورة إيجـاد بنيـة تشريـعية عربيـة ملائمـة، وإيجـاد بنيـة تحتية قوية من وسـائل الاتصـال الحديثـة والشـبكات اللازمـة لتزويـد خـدمات شـبكة الإنترنت ومراكز الأبحاث والتـدريب، واعتمـاد المعلومــات والبيانـات العمليـة في حيـاة المجتمع، وبناء قاعدة معلومات لتبادل المعلومات بـين الـدول العربيـة، وزيـادة الخـبرات لزيادة حجم التجارة الإلكترونية البينية على المستويين الوطني والقومي، والعمل على رفع مستوى التعليم في مجال المعلوماتية، وبناء المجتمع القادر عـلى اسـتيعاب فكـرة التجـارة الإلكترونية وتقبلها، والتغلب على مخاطرها بالوسائل التقنية والقانونية، وتـوفير الخـبرات في مجال اسـتخدام تكنولوجيـا المعلومـات وصـيانة الأجهـزة والشـبكات، وزيـادة الـوعي وتعميـق مفهوم المجتمع بأهمية التجارة الإلكترونيـة، والاسـتفادة منهـا بالشـكل الأمثـل، والعمل على تدريس موضوع التجارة الإلكترونية في كليات القانون في الدول

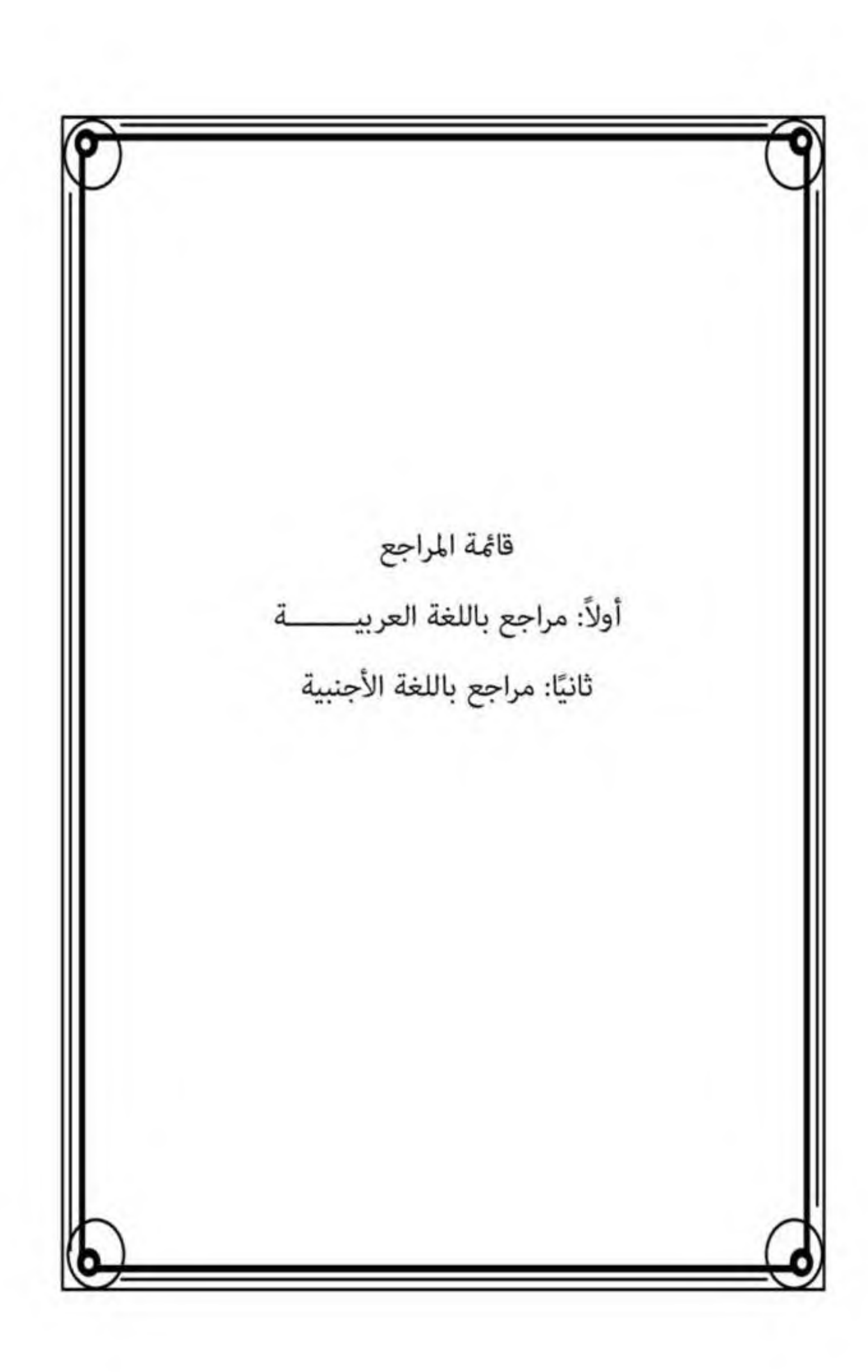
العربية.

9) **التوصية التاسعة:** العمل على سرعة إعداد معاهدة دولية تكون إطارًا لنظام قانوني موحد للتجارة الإلكترونية على مستوى العالم، من أجل إزالة العوائق وتخفيض التكاليف بالنسبة للشركات التي تستخدم شبكة الإنترنت لإدارة الأعمال التجارية، وزيادة الثقة بالتجارة الإلكترونية خصوصًا فيما يتعلق بعقد الصفقات الإلكترونية وتبادل البيانات والرسائل البريدية الإلكترونية، على أن تشمل تلك المعاهدة إطارًا لنظام قانوني موحد لحل النزاعات المتعلقة بالتجارة الإلكترونية بما يضمن أمن وخصوصية هذه التجارة.

10) **التوصية العاشرة:** ضرورة التنسيق الدولي في السياسات الجنائية من أجل وضع معاهدة دولية لمكافحة جرائم تقنية المعلومات، ومتابعة مرتكبي هذه الجرائم، على غرار اتفاقية بودابست، تتناول الجانب الموضوعي والذي يتناول الجرائم بكافة أشكالها، والجانب الإجرائي والذي يتضمن إجراءات التفتيش والضبط في العالم الافتراضي، والتعاون الدولي في هذا المجال، والعمل على تأهيل وتدريب القائمين على مكافحة الجريمة المعلوماتية.

تم بحمد الله تعالى





قائمة المراجع

أولاً: مراجع باللغة العربيـــــــة

ثانيًا: مراجع باللغة الأجنبية

أولاً: مراجع باللغة العربية

الكتب:

(1) د. أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية،2000.

(2) ـــــــ الحماية الجنائية للحاسب الآلي، دار النهضة العربية,2000.

(3) د. أحمد شرف الدين، عقود التجارة الإلكترونية -تكوين العقد وإثباته، دار النهضة العربية، 2000.

(4) د. أحمد عبد الكريم سلامة، القانون الدولي الخاص النوعي (الإلكتروني، السياحي، البيئي)، دار النهضة العربية، الطبعة الأولى، 2002.

(5) د. أحمد عوض بلال، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة، 2007.

(6) د. أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1979.

(7) د. أسامة أبو الحسن مجاهد، خصوصية التعاقد عبر الإنترنت، دار الكتب القانونية، 2002.

(8) د. أسامة أحمد بدر، بعض مشكلات تداول المصنفات عبر الإنترنت، دار النهضة العربية، 2002.

(9) د. أسامة عبد الله قايد، الحماية الجنائية لحق المؤلف، الطبعة الأولى، دار النهضة العربية، القاهرة، 1991.

(10) د. أسامة محمد محيي الدين، مدخل الحاسب الآلي ونظم

المعلومات، ج 1، مقدمة الحاسب الآلي، ط 1، دار القلم، دبي، 1990.

(11) د. أشرف شمس الدين، الحماية الجنائية للمستند الإلكتروني، ط 1، القاهرة، دار النهضة العربية، 2006.

(12) أيمن العشري، المرجع في أساسيات الحاسب الآلي للمبتدئين، 1997

(13) أيمن عبد الحفيظ، الاتجاهات الفنية لمواجهة الجرائم المعلوماتية، دار النهضة العربية، 2005.

(14) د. إيهاب السنباطي، الترجمة الجديدة والكاملة للاتفاقية المتعلقة بالجريمة الإلكترونية (بودابست 200 والبروتوكول الملحق بها، 2009

(15) د. السعيد مصطفى السعيد، قانون العقوبات، القسم الخاص، دار المعارف, القاهرة.

(16) ـــــــــــــ، قانون العقوبات، القسم العام،، دار المعارف, القاهرة

(17) د. السيد أحمد عبد الخالق، الأهمية الاقتصادية للتجارة الإلكترونية، جامعة المنصورة، دون سنة نشر.

(18) ـــــــــــــ، التجارة الإلكترونية والعولمة، المنظمة العربية للتنمية الإدارية، 2006.

(19) د. السيد عتيق، جرائم الإنترنت، دار النهضة العربية، القاهرة، 2000 ص120.

(20) برنارد أ. جالر، الملكية الفكرية وبرامج الحاسبات، الجمعية المصرية لنشر المعرفة والثقافة العالمية، 1998.

(21) د. توفيق حسن فرج، المدخل للعلوم القانونية، مكتبة مكاوي،

بيروت، 1975

(22) د. ثروت عبد الحميد، التوقيع الإلكتروني، مكتبة الجلاء الجديدة، المنصورة، 2001.

(23) ـــــــ التوقيع الإلكتروني، ماهيته، مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات، دار الجامعة الجديدة، 2004.

(24) د. جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول, الجرائم الناشئة عن استخدام الحاسب الآلي, دار النهضة العربية، القاهرة، 1992.

(25) ـــــــ الإنترنت والقانون الجنائي، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 1999.

(26) ـــــــ الحماية الجنائية والمدنية لبطاقات الائتمان، دار النهضة العربية، القاهرة، 1999.

(27) ـــــــ مقدمة في الحاسب الآلي، (دراسة عملية ونظري)، دار النهضة العربية، القاهرة، 1999/ 2000.

(28) جندي عبد الملك، الموسوعة الجنائية، ج4، دار الكتب المصرية.

(29) د. حسن صادق المرصفاوي، قانون العقوبات الخاص، منشأة المعارف، الإسكندرية، 1991،

(30) حسن طاهر داود، أمن شبكات المعلومات، مركز البحوث، معهد الإدارة العامة، الرياض، 2004.

(31) د. حسن عبد الباسط جميعي، إثبات التصرفات التي يتم إبرامها عن طريق الإنترنت, دار النهضة العربية, طبعة 2000.

(32) د. حسن كيرة، المدخل إلى القانون، دار النهضة العربية، بيروت،

.1967

(33) د. حسني الجندي, التشريعات الجنائية الخاصة في دولة الإمارات العربية المتحدة, قانون مكافحة جرائم تقنية المعلومات, بدون ناشر, 2009.

(34) حسين الغافري ومحمد الألفي، جرائم الإنترنت بين الشريعة الإسلامية والقانون، دار النهضة العربية، 2008.

(35) د. حسين بن سعيد الغافري, السياسة الجنائية في مواجهة جرائم الإنترنت, دار النهضة العربية, 2009.

(36) د. حمد الله محمد حمد الله، مختارات من قانون الاستهلاك الفرنسي، دار النهضة العربية، القاهرة، 2000.

(37) خاطر لطفي، الموسوعة الشاملة في قوانين حماية حق المؤلف والرقابة على المصنفات الفنية، 1994.

(38) د. خالد حمدي عبد الرحمن، التعبير عن الإرادة في العقد الإلكتروني، دار النهضة العربية، 2007.

(39) د. خالد محمد المهيرى، النظام القانوني للتجارة الإليكترونية في دولة الإمارات العربية المتحدة، ط. ثانية، معهد القانون الدولي، دبي، 2004

(40) د. رءوف عبيد، جرائم الاعتداء على الأشخاص والأموال، دار الفكر العربي، القاهرة، 1978.

(41) د. رمسيس بهنام، شرح قانون العقوبات، القسم الخاص، 1982.

(42) ـــــ، الجريمة والمجرم في الواقع الكوني، منشأة المعارف، الإسكندرية 1996.

(43) سامر محمد سعيد، الإنترنت المنافع والمحاذير، دار سعاد الصباح،

الكويت 1988.

(44) د. سامي عبد الباقي أبو صالح، التحكيم التجاري الإلكتروني دراسة مقارنة، دار النهضة العربية، 2004.

(45) د. سعيد السيد قنديل، التوقيع الإلكتروني، ماهيته، صوره، حجيته في الإثبات بين التدويل والاقتباس، دار الجامعة الجديدة للنشر، الإسكندرية،2004.

(46) د. سمير حامد عبد العزيز الجمال، التعاقد عبر تقنيات الاتصال الحديثة، دار النهضة العربية، القاهرة، 2006.

(47) د. شحاتة غريب محمد شلقامي، الحق الأدبي لمؤلف برامج الحاسب الآلي، دراسة في قانون حماية الملكية الفكرية الجديد رقم 82 لسنة 2002، دار الجامعة الجديدة، القاهرة، 2008.

(48) د. شريف محمد غانم، حماية العلامات التجارية عبر الإنترنت في علاقتها بالعنوان الإلكتروني، دار النهضة العربية، القاهرة، دون سنة نشر.

(49) د. شيماء عبد الغني عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، 2007م.

(50) د. طارق عبد العال، التجارة الإلكترونية، الدار الجامعية، الإسكندرية، 2005.

(51) د. طارق فتحي سرور، دروس في جرائم النشر، دار النهضة العربية، 1997.

(52) د. طاهر شوقي مؤمن، عقد البيع الإلكتروني، بحث في التجارة الإلكترونية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2008

(53) د. عبد الأحد جمال الدين، النظرية العامة للجريمة، دار الثقافة

الجامعية، القاهرة، 1993.

(54) د. عبد الرازق السنهوري، الوسيط في شرح القانون المدني العربي، المجلد الثامن، حق الملكية، دار إحياء التراث، بيروت

(55) د. عبد السميع عبد الوهاب أبو الخير، الحق المالي للمؤلف في الفقه الإسلامي والقانوني المقارن، مكتبة وهبة، القاهرة، 1988.

(56) د. عبد العظيم مرسي وزير, شرح قانون العقوبات، القسم الخاص، جرائم الاعتداء على الأموال , دار النهضة العربية، القاهرة، 1993.

(57) د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الكتب القانونية، المحلة الكبرى، 2001.

(58) ـــــــــــ النظام القانوني لحماية التجارة الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2002.

(59) ـــــــــــ مقدمة في التجارة الإلكترونية العربية، ط ثانية، دار الفكر الجامعي، الإسكندرية، 2003.

(60) ـــــــــــ الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، 2003.

(61) ـــــــــــ التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، 2004.

(62) ـــــــــــ التوقيع الإلكتروني في النظم القانونية المقارنة، دار الفكر الجامعي، الإسكندرية 2005، ط أولى.

(63) ـــــــــ، مكافحة جرائم الكمبيوتر والإنترنت في القانون العربي النموذجي، دراسة متعمقة في القانون المعلوماتي، دار الفكر الجامعي، الإسكندرية، 2006.

(64) ـــــــــ، الحكومة الإلكترونية ونظامها القانوني، المجلد الثاني، دار الفكر الجامعي، الإسكندرية، 2006.

(65) ـــــــــ، الإثبات الجنائي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، مصر، 2007.

(66) ـــــــــ، جرائم الكمبيوتر والإنترنت في التشريعات العربية، دار النهضة العربية، القاهرة، 2009.

(67) د. عبد الفتاح مراد، التجارة الإلكترونية والبيع والشراء على شبكة الإنترنت، الهيئة القومية لدار الكتب والوثائق المعدلة، القاهرة، 2004.

(68) د. عبد المنعم فرج الصدة، محاضرات في القانون المدني، حق المؤلف في القانون المصري، مطبوعات جامعة الدول العربية، معهد البحوث والدراسات العربية، القاهرة، 1967.

(69) د. عبد المهيمن بكر سالم، جرائم الاعتداء على الأشخاص والأموال، 1977.

(70) د. عصام أنور سليم، خصائص البيع الدولي وفقا لاتفاقية الأمم المتحدة بشأن البيع الدولي للبضائع المبرمة في فيينا سنة 1998،منشأة المعارف، الإسكندرية، 2004.

(71) د. عطا عبد العاطي محمد السنباطي، موقف الشريعة الإسلامية من جرائم الحاسب الآلي، دراسة مقارنة، دار النهضة

العربية،2002.

(72) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة، دراسة مقارنة،جامعة الإسكندرية، 2000

(73) د. علي بن عبد الله عسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، المملكة العربية السعودية، 2004.

(74) د. علي جمال الدين عوض, الاعتمادات المستندية, دراسة للقضاء والفقه المقارن وقواعد سنة 1983 الدولية, دار النهضة العربية، القاهرة، 1989.

(75) د. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 1997.

(76) د. عمر السعيد رمضان، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1986.

(77) د. عمر سالم، الحماية الجنائية لبطاقات الوفاء، دار النهضة العربية، 1995.

(78) د. عمر محمد أبو بكر بن يونس، المجتمع المعلوماتي والحكومة الإلكترونية، موسوعة التشريعات العربية، 2003.

(79) ـــــــــ الجرائم الناشئة عن استخدام الإنترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، 2004.

(80) ـــــــــ الإيكان, دار النهضة العربية, 2005.

(81) ـــــــــ الحماية الجنائية للثروة النفطية، دار

الفكر الجامعي، 2004.

(82) ــــــــــــ الاتفاقية الأوروبية حول الجريمة الافتراضية (المذكرة التفسيرية)، بدون ناشر، 2005.

(83) ــــــــــــ الدليل الرقمي، الجمعية العربية لقانون شبكة الإنترنت، 2008.

(84) عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات - دراسة مقارنة - دار النهضة العربية، القاهرة 2000

(85) د. عوض محمد عوض، جرائم الأشخاص والأموال، دار المطبوعات الجامعية، الإسكندرية، 1984.

(86) ــــــــــــ قانون العقوبات، القسم الخاص، دار المطبوعات الجامعية، 1991.

(87) د. فاروق الأباصيري، عقد الاشتراك في قواعد المعلومات عبر شبكة الإنترنت، دار الجامعة الجديدة، 2002.

(88) د. فاروق حسين، البريد الإلكتروني، الهيئة العامة للكتاب، 1999.

(89) فاروق علي الحفناوي، قانون البرمجيات، دار الكتاب الحديث، 2001.

(90) فريد هـ كيت، الخصوصية في عصر المعلومات، ترجمة محمد محمود شهاب، بدون ناشر، 2000.

(91) د. فوزية عبد الستار، شرح قانون العقوبات، القسم الخاص، دار النهضة العربية، 1988.

(92) قانون الأونسيترال النموذجي بشأن التجارة الإلكترونية مع دليل التشريع، مطبوعات الأمم المتحدة، نيويورك 2000.

(93) مجموعة من الخبراء، المعاملات الرقمية وقانون شبكة الإنترنت،

المنظمة العربية للتنمية الإدارية، 2006.

(94) د. محمد أبو العلا عقيدة، الاتجاهات الحديثة في قانون العقوبات الفرنسي- الجديد، دار النهضة العربية، 1997.

(95) محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، دار المطبوعات الجامعية، الإسكندرية، 2003.

(96) محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، دار الثقافة ل لنشر والتوزيع، عمان، 2004.

(97) د. محمد السعيد رشدي، شبكة الإنترنت والجوانب القانونية لنظم المعلومات، مؤسسة دار الكتب للطباعة والنشر والتوزيع، الكويت، 1997.

(98) ـــــــ حجية وسائل الاتصال الحديثة في الإثبات، النسر الذهبي للطباعة، بدون سنة طبع.

(99) د. محمد الصيرفي، التجارة الإلكترونية، مؤسسة حورس الدولية، مصر، 2005.

(100) د. محمد المرسي زهرة، حجية التوقيع الإلكتروني في الإثبات، بدون ناشر, وبدون سنة طبع.

(101) محمد بن راشد آل مكتوم, رؤيتي التحديات في سباق التميز,موتيفيت للنشر, 2006.

(102) د. محمد حسام لطفي، الحماية القانونية لبرنامج الحاسب الآلي، دار الثقافة العربية، 1987.

(103) ـــــــ استخدام وسائل الاتصال الحديثة في التفاوض على العقود وإبرامهما، بدون ناشر، القاهرة، 1993.

(104) ـــــــ الإطار القانوني للمعاملات الإلكترونية، مطبعة النسر- الذهبي، القاهرة، 2002.

(105) د. محمد حسني عباس، الملكية الصناعية والمحل التجاري، دار النهضة العربية، القاهرة، 2000.

(106) د. محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، طبعة 2003.

(107) د. محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998.

(108) د. محمد عبد الظاهر حسين، المسئولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، 2002.

(109) محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.

(110) محمد محرم محمد علي، خالد محمد كدفور المهيري، قانون العقوبات الاتحادي، الفتح للطباعة والنشر، 19928.

(111) د. محمد مراد عبد الله، شبكة الإنترنت وجناح الأحداث، الأمن والإنترنت، القيادة العامة لشرطة دبي، 2001.

(112) د. محمود السيد عبد المعطي خيال، الإنترنت وبعض الجوانب القانونية، دار النهضة العربية، القاهرة، دون سنة نشر.

(113) د. محمود محمود مصطفى، شرح قانون العقوبات، القسم العام، الطبعة العاشرة، دار النهضة العربية، القاهرة، 1984.

(114) ـــــــ الجرائم الاقتصادية في القانون المقارن، الأحكام العامة والإجراءات الجنائية، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، دون سنة نشر.

(115) د. محمود نجيب حسني، شرح قانون العقوبات، القسم الخاص، الجرائم المضرة بالمصلحة العامة، 1972.

(116) ـــــــــ شرح قانون العقوبات، القسم العام، القاهرة، دار النهضة العربية، 1977.

(117) ـــــــــ جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، دراسة مقارنة،1984.

(118) ـــــــــ النظرية العامة للقصد الجنائي، دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، 1988.

(119) د. مدحت عبدالحليم رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2000.

(120) ـــــــــ الحماية الجنائية للتجارة الإلكترونية, دار النهضة العربية، 2001

(121) د. مصطفى الجمال، والدكتور عبد الحميد الجمال، مبادئ القانون، الكتاب الثاني، العلاقات القانونية، الفتح للطباعة والنشر، الإسكندرية، 1992.

(122) مصطفى السيد، دليلك إلى شبكة الإنترنت، دار الكتب العلمية، 2000.

(123) د. مصطفى المصمودي، المجتمع المدني العربي في زمن الثورة الرقمية، دار البستان للنشر، تونس، نوفمبر 2005.

(124) د. مصطفى منير السيد، جرائم استعمال السلطة الاقتصادية، الهيئة المصرية العامة للكتاب، القاهرة، 1992.

(125) د. ممدوح عبد الحميد، جرائم استخدام الكمبيوتر وشبكة المعلومات العالمية، دار الحقوق، الشارقة، 2001.

(126) منير محمد الجنبيهي، ممدوح محمد الجنبيهي، التوقيع الإلكتروني وحجيته في الإثبات، دار الفكر الجامعي، الإسكندرية، 2004.

(127) ـــــــــــ، ـــــــــــ، قوانين الأونسيترال النموذجية في مجال التجارة الإلكترونية، دار الفكر الجامعي، 2006.

(128) د. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، 2004.

(129) د. نزيه محمد الصادق المهدي، النظرية العامة للالتزام، دراسة نظرية تطبيقية في مبادئ الإثبات، دار النهضة العربية، القاهرة، 2001.

(130) د. هاني عبد السلام أحمد، الجوانب الموضوعية والإجرائية للجرائم المعلوماتية، دار النهضة العربية، 2003.

(131) د. هدى حامد قشقوش، جرائم الحاسب الآلي في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

(132) ـــــــــــ، الإتلاف العمدي لبرامج الحاسب الآلي، دار النهضة العربية، القاهرة، 1997.

(133) ـــــــــــ، الحماية الجنائية للتجارة الإلكترونية عبر الإنترنت، دار النهضة العربية، 2000.

(134) د. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.

(135) د. هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست، دار النهضة العربية، 2003

(136) ـــــــــــ، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2006.

(137) ــــــــــ: اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، 2007.

(138) ــــــــــ، جرائم المعلومات عبر الحدود وأساليب مواجهتها وفق اتفاقية بودابست، دار النهضة العربية، القاهرة، 2008.

(139) د. وليد عودة، الموسوعة الحاسوبية، الإصدار الأول،2003.

(140) د. يسر أنور علي، شرح قانون العقوبات، القاهرة، 1993.

المؤتمرات والندوات:

(141) د. إبراهيم الدسوقي أبو الليل، توثيق التعاملات الإلكترونية ومسئولية جهة التوثيق تجاه الغير، مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي من 10: 12 مايو 2003، إدارة المطبوعات، جامعة الإمارات، المجلد الخامس5.

(142) د. أحمد شرف الدين، الجوانب القانونية للتجارة الإلكترونية وآليات حل منازعاتها، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون وغرفة تجارة وصناعة دبي 10: 12 مايو 2003.

(143) د. أماني قنديل، ندوة (مستقبل مؤسسات المجتمع المدني في دول مجلس التعاون الخليج 3، 4 أبريل 2000، مركز جامعة الخليج والجزيرة العربية (جامعة الكويت).

(144) د. بلال عبد المطلب بدوي، البنوك الإلكترونية، البنوك الإلكترونية ماهيتها, معاملاتها, المشاكل التي تثيرها, مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون, كلية الشريعة

والقانون وغرفة تجارة وصناعة دبي, 10: 12 مايو 2003, إدارة المطبوعات، جامعة الإمارات, المجلد الخامس.

(145) د. حسام الدين الأهواني، حماية حقوق الملكية الفكرية، مؤتمر حول الملكية الفكرية، جامعة اليرموك الأردن، 10 تموز 2000.

(146) د. حسن الماحي، نظرات قانونية في التجارة الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، في الفترة من 26: 28 أبريل 2003.

(147) د. حسن عبد الباسط جميعي، الحماية القانونية لمواقع الإنترنت وأسماء الدومين، بحث مقدم لندوة الويب الوطنية عن الملكية الفكرية التي نظمتها المنظمة العالمية للملكية الفكرية الوايبو بالتعاون مع جامعة القاهرة (مصر- في الفترة من 17 إلى 19 فبراير 2003.

(148) د. سليمان بن محمد الشدي، الجانب التشريعي والقضائي في دول مجلس التعاون لدول الخليج العربية ودوره في دعم التعاملات والتجارة الإلكترونية، المؤتمر العلمي السنوي السابع عشر المعاملات الإلكترونية (التجارة الإلكترونية - المعاملات الإلكتروني 19-20/ مايو 2009، تنظيم جامعة الإمارات العربية المتحدة، مركز البحوث والدراسات الإستراتيجية.

(149) د. سمير برهان، إبرام العقد في التجارة الإلكترونية بحث مقدم إلى مؤتمر الجوانب القانونية للتجارة الإلكترونية، والمنعقد بالقاهرة في الفترة 12، 13 يناير 2002.

(150) د. عبد الفتاح بيومي حجازي، حماية المستهلك في عقود التجارة

الإلكترونية، بحث مقدم إلى مؤتمر حماية المستهلك المنعقد لدى الأمانة العامة لدول مجلس التعاون الخليجي بالرياض مع غرفة التجارة والصناعة بالرياض، في الفترة 18، 19 سبتمبر 2004، منشور في كتاب "مقدمة في الملكية الفكرية وحماية المستهلك"، دار الفكر الجامعي، الإسكندرية، 2005.

(151) د. علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة إلكترونيا، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، العين، 1 - 3 مايو 2000.

(152) ــــــــ جرائم التعدي على نظام معالجة المعطيات، بحث مقدم لمؤتمر القانون الكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، مايو 2000.

(153) ــــــــ: الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، بحيث مدم لمؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، دبي الإمارات العربية المتحدة / 26 - 28 أبريل 2003

(154) د. عمر الفاروق الحسيني، لمحة عن جرائم السرقة من حيث اتصالها بنظم المعالجة الآلية للمعلومات، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت, جامعة الإمارات, 1-3 مايو 2000

(155) د. غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من1، 3 مايو2000.

(156) ــــــــ، بحث عن العلاقة بين الاحتيال والإجرام

المنظم، مقدم لندوة الاحتيال والإجرام المنظم التي نظمتها جامعة نايف مع كلية الحقوق بجامعة المنصورة.

(157) فتحي محمد عبد الغني، مقدمة إلى التجارة الإلكترونية وتطوراتها، ورقة عمل مقدمة للندوة الأولى حول التجارة الإلكترونية (نماذج اليونسترا، الإسكندرية 9: 12 أبريل 2006.

(158) د. فياض ملفي القضاة، مسئولية البنوك الناتجة عن استخدام الكمبيوتر كوسيلة وفاء، مؤتمر القانون والكمبيوتر والإنترنت،جامعة الإمارات, المجلد الأول.

(159) د. كامران الصالحي, الطبيعة القانونية لمسئولية خدمات التصديق, مؤتمر المعاملات الإلكترونية (التجارة الإلكترونية, الحكومة الإلكتروني 19- 25 مايو 2009, جامعة الإمارات, مركز الإمارات للبحوث والدراسات الإستراتيجية, ج2.

(160) د. محمد أبو العلا عقيدة, الحماية الجنائية للتجارة الإلكترونية, مؤتمر مكافحة جرائم تقنية المعلومات, جامعة الشارقة, كلية القانون 26-30 نوفمبر 2006.

(161) د. محمد السيد عرفة، التجارة الدولية الإلكترونية عبر شبكة الإنترنت ومفهومها والقاعدة القانونية التي تحكمها ومدى حجية المخرجات في الإثبات، بحث مقدم إلى مؤتمر القانون والكمبيوتر، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة، الفترة من 1: 3 مايو 2000.

(162) د. محمد حسام لطفي، النظام القانوني لحماية الحقوق الذهنية في مصر، بحث منشور في كتاب ندوة حقوق المؤلف الفكرية في مصر

(163) د. محمد سامي الشوا، الغش المعلوماتي كظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25: 28 أكتوبر 1993.

(164) د. محمد عفيفي حمودة, مفهوم حماية المستهلك, بحث مقدم في ندوة حماية المستهلك نظمتها لجنة العلوم الإدارية بالمجلس الأعلى للثقافة بالقاهرة في 23 يونيه عام 1981.

(165) د. محمود أحمد إبراهيم الشرقاوي, مفهوم الأعمال المصرفية الإلكترونية واهم تطبيقاتها, بحث مقدم إلى مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، جامعة الإمارات، كلية الشريعة والقانون، 10-12 مايو 2003

(166) د. نائل عبد الرحمن صالح، واقع جرائم الحاسوب في التشريع الأردني، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات، مايو 2000.

(167) د. هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، بحث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي بعنوان [الجرائم الواقعة في مجال تكنولوجيا المعلومات] القاهرة، 25- 28 أكتوبر 1993، دار النهضة المصرية.

(168) وليد عالكوم، مفهوم ظاهرة الإجرام المعلوماتي، بحث مقدم في مؤتمر القانون والكمبيوتر والإنترنت، كلية الشريعة والقانون، جامعة الإمارات العربية، 2000.

(169) يونس عرب، جرائم الكمبيوتر والإنترنت، إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة

والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002، تنظيم المركز العربي للدراسات والبحوث الجنائية، أبو ظبي 10 - 12 /2002/2.

الرسائل العلمية والأبحاث:

(170) د. إبراهيم أبو الهيجاء، القانون الواجب التطبيق على عقود التجارة الإلكترونية، رسالة دكتوراه، حقوق القاهرة، 2004.

(171) د. أمين أعزان، الحماية الجنائية للتجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس.

(172) د. أيمن عبد الله فكري، جرائم نظم المعلومات دراسة مقارنة، رسالة دكتوراه جامعة المنصورة، كلية الحقوق، 2006.

(173) د. بضراني نجاة, الائتمان المصرفي بطريق التوقيع (الاعتماد بالقبول, الكفالة المصرفية, خطاب الضما, رسالة دكتوراه, كلية الحقوق، جامعة القاهرة, 1987.

(174) بيتر آن جرابسكي، الجريمة في فضاء شبكة الإنترنت، بحث منشور ضمن سلسلة الأمن والإنترنت، مركز بحوث شرطة دبي.

(175) بيل جيتس، المعلوماتية بعد شبكة الإنترنت (طريق المستقبل) ترجمة عبد السلام رضوان، سلسة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، مارس 1998.

(176) د. حسين بن سعيد بن سيف الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007.

(177) د. خالد إبراهيم ممدوح، إبرام العقد الإلكتروني، رسالة دكتوراه، جامعة الإسكندرية، 2005.

(178) د. خالد حمدي عبد الرحمن، الحماية القانونية للكيانات المنطقية، رسالة دكتوراه، جامعة عين شمس، 1992.

(179) د. طوني ميشال عيسى، التنظيم القانوني لشبكة الإنترنت، رسالة دكتوراه، بيروت 2000.

(180) د. عايض راشد عايض المري، مدى حجية الوسائل التكنولوجية الحديثة في إثبات العقود، رسالة دكتوراه، جامعة القاهرة، 1998.

(181) د. عبادة أحمد عبادة, التدمير المتعمد لأنظمة المعلومات الإلكترونية, منشورات مركز البحوث والدراسات, شرطة دبي, مارس 1999.

(182) د. عبد الحفيظ بالقاضي، مفهوم حق المؤلف وحدود حمايته جنائيًا، رسالة دكتوراه، كلية الحقوق، الرباط، دار الأمان، المغرب، 1995.

(183) د. عصام فايد، مسئولية البنك عن فحص المستندات في الاعتماد المستندي، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 2007.

(184) فادي محمد عماد الدين توكل، عقد التجارة الإلكترونية، رسالة ماجستير مقدمة لكلية الحقوق جامعة القاهرة، دار النهضة العربية، 2008.

(185) د. فهد بن سيف بن راشد الحوسني، جرائم التجارة الإلكترونية ووسائل مواجهتها مع التطبيق على سلطنة عمان، رسالة دكتوراه مقدمة إلى أكاديمية الشرطة، مصر، 2007.

(186) د. مأمون محمد سلامة، بحث بعنوان قانون العقوبات بين الفكر المحافظ والفكر المتطور، دراسات قانونية, كلية الحقوق, الجامعة الليبية, 1971.

(187) د. محمد أحمد محمد نور جستنية، مدى حجية التوقيع الإلكتروني في عقود التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 2005.

(188) د. محمد سعيد أحمد إسماعيل، أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005.

(189) د. محمد نور الدين سيد، المسئولية الجنائية عن الاستعمال غير المشروع لبطاقات الوفاء، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2005.

(190) د. ميرفت عبد المنعم صادق، الحماية الجنائية للمستهلك، رسالة دكتوراه، حقوق القاهرة، 1999.

(191) د. نافذ ياسين محمد المدهون، النظام القانوني لحماية التجارة الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007.

(192) هند محمد حامد، التجارة الإلكترونية في المجال السياحي، رسالة ماجستير، كلية السياحة والفنادق، جامعة حلوان.

الدوريات:

(193) د. إبراهيم أحمد إبراهيم، التجارة الإلكترونية والملكية الفكرية، مجلة المحاماة، العدد الأول، 2001.

(194) د. أسامة الخولي، الحاسوب هذا الطفل الذي ولد كبيراً، مجلة عالم الفكر الكويتية، عدد أكتوبر، نوفمبر، ديسمبر 1987.

(195) د. أسامة مجاهد، استخدام الحاسب الآلي في المجال القضائي, مجلة القضاة، عدد يناير، يونيو 1990.

(196) جوجيو ديلفيكيو مقال بعنوان: فلسفة القانون في إيجاز، ترجمة د. ثروت أنيس الأسيوطي، منشور بمجلة القانون والاقتصاد، الصادرة عن كلية الحقوق جامعة القاهرة، السنة 12 / 1972، العدد الأول.

(197) د. حسام الأهواني، الحاسب الآلي والحياة الخاصة بحث منشور في مجلة العلوم والاقتصاد، كلية الحقوق، جامعة عين شمس، عدد يناير، 1990.

(198) حسن الحفني، التجارة الإلكترونية في الوطن العربي الفرص والتحديات، سلسلة دراسات اقتصادية، مركز الخليج للدراسات الإستراتيجية، مايو 2002.

(199) د. حمدي عبد العظيم، أبعاد التجارة الإلكترونية، مجلة البحوث الإدارية، العدد الأول، يناير 2001.

(200) رأفت رضوان, عالم التجارة الإلكترونية, المنظمة العربية للتنمية الإدارية، القاهرة، مجلة سلسلة بحوث ودراسات, العدد 348, 1999.

(201) د. سهير حجازي، التهديدات الإجرامية للتجارة الإلكترونية، مجلة بحوث ودراسات شرطية، شرطة دبي، العدد91، 1999.

(202) د. صفوت عبد السلام عوض الله، تحرير تجارة الخدمات في ظل اتفاقية الجات وانعكاساتها على اقتصاديات الدول النامية، مجلة العلوم القانونية والاقتصادية، العدد الأول، سنة 40، يناير 1998.

(203) د. عبود السراج، الجريمة في إطار التفسير الاقتصادي للمجتمع، مجلة الحقوق والشريعة، العدد الثاني السنة الثالثة، الكويت 1979.

(204) د. هيفاء أيوب ججاوي، الأسلوب العلمي في تقييم قواعد البيانات من وجهة نظر المكتبيين، المجلة العربية للمعلومات، المنظمة

العربية للتربية والعلوم والثقافة، 2000.

وثائق وتقارير:

(205) د. إبراهيم أحمد، تقرير عن الجوانب القانونية للتجارة الإلكترونية في مصر، تقرير مقدم لمركز المعلومات ودعم اتخاذ القرار، القاهرة، 2000.

(206) إعلان القاهرة، الوثيقة العربية، نحو مجتمع معلومات عربي، خطة العمل المشترك، القاهرة في 18 يونيو "حزيران" 2003.

(207) الوثيقة العربية لقانون شبكة الإنترنت الصادرة عن المؤتمر الدولي الأول لقانون شبكة الإنترنت الغردقة 21: 25 أغسطس 2005.

أبحاث منشورة على شبكة المعلومات:

(208) د. أمجد حسان، الفيروسات إرهابا تهدد أنظمة المعلومات، مقال مقدم إلى ملتقى الإرهاب في العصر الرقمي، جامعة الحسين بن طلال، عمان، 10 - 12 يوليو 2007. ومتوفر على العنوان التالي: www.ahu.edu.jo/tda/papers%5C89.doc

(209) جميل حلمي، مقال بعنوان الحماية الإلكترونية للمستهلك، منشور على شبكة الإنترنت: www.al3ez.net/vb/showthread

(210) خالد بن نواف الحربي، الأمن والحماية في شبكة الإنترنت للمستخدم العربي، منشور على شبكة الإنترنت: http://www.boosla.com/

(211) د. رأفت عبد العزيز غنيم، دور جامعة الدول العربية في تنمية وتيسير التجارة الإلكترونية بين الدول العربية، نوفمبر 2002. بحث منشور على الموقع التالي: www.ebi.org.eg/E.../Role%20of%20Arab%20League

%20in%20development%2...

(212) د. فؤاد جمال عبد القادر، إطلالة على مشروع قانون التجارة الإلكترونية، منشور على شبكة الإنترنت بالموقع: http://www.tashreaat.com

(213) د. محسن محمد العبودي، كارثة فيروسات الكمبيوتر والجرائم المتعلقة بالإنترنت، بحث منشور على شبكة الإنترنت www.arablawinfo.com.

(214) محمد محرم محمد علي، جريمة النصب والتجارة لإلكترونية، بحث منشور على شبكة الإنترنت على الموقع:

http://www.arablaw.org/Research%20&%20Studys.htm

(215) يونس عرب، التجارة الالكترونية، بحث منشور على شبكة الانترنت على الموقع:- doc.abhatoo.net.ma/IMG/doc/dro8.doc

(216) يونس عرب، أمن المعلومات ماهيتها وعناصرها وإستراتيجياتها، بحث منشور على شبكة الإنترنت www.arablaw.org

(217) **يونس عرب، البنوك الخلوية، التجارة الخلوية، المعطيات الخلوية،M ، banking, data،commerce, M،M، ثورة جديدة تنبئ بانطلاق عصر ما بعد المعلومات، بحث منشور على شبكة الإنترنت، http://www.arablaw.org**

ثانيا: مراجع باللغة الأجنبية

مراجع باللغة الإنجليزية:

(1) Alan M Gahtan, Electronic Evidence, Thomas Canada Limited 1999.

(2) Alex Birch& Others, the age of E, conquering the new world of electronic shopping, U K:OC &C and the McKenna Group, 2000.

(3) American Network, Inc. v. Access America/Connect Atlanta, Inc. (SDNY, Decided, August 13, 199 at: http://www.ipcounselors.com/19970922.htm#a3

(4) Angel J: Why use Digital signatures for Electronic commerce? Commentary 1999, the journal of information, Law and Technology (JIL , p3 "http://eli.warwick.ac.uk\Jilt\199, 2\angel.html"

(5) Bernard D. Reams. JR, Electronic Contracting Law, EDI and Business Transaction , Clark board man Callaghan , 1997 p32.

(6) Catherine L. Mann & Sue E. Eckert, Global Electronic Commerce, Institute for international Economic, A policy Primer, Washington Dc, 2000.

(7) Charles Chatterjee, Ecommerce law for Business Managers, Financial World publishing, London, 2002.

(8) Clive Gringras, The laws of the internet, Butter worth's press London 1997.

(9) Consumer contracts are those concluded between a merchant and a consumer, this latter generally being a private person who contracts for purposes outside of his or her trade or profession. (Council Directive, 13/93, 5 April 199.

(10) David L. Hayes, Advanced Copyright Issues On The Internet, Part Viii, Computer Law & Security

Report Vol. 18 No. 1, 2002.

(11) David U. Haltinner Sentenced To 50 Months Of Imprisonment For Selling Approximately 637,000 Stolen Credit Card Numbers.

(12) Drury.Ac.Ferrier ,CW Ccredit Card , London, Butter Wrth 1984.

(13) Efraim Turban & Jae Lee & David King & H.Michael Chung, Electronic Commerce A Managerial Perspective, Prentice Hall, Inc, New Jersey, 2000.

(14) Ejan Mackaay & Daniel Poulin, The Electronic Super Highway, The shape of Technology and Law to come Kluwer Law International 1995.

(15) Eric. J. sinord & Barak D.jolish. controlling chaos: the emerging law of privacy and speech in cyberspace. Stanford technology law review, vol. 1 1999.

(16) European commission: Digital signatures A survey of law and practice in the European union, Wood DHEAD publishing LIMITED, Cambridge England, 2001

(17) Indira Carr & Katherine S Williams, Securing The E, Commerce Environment Enforcement Measures And Penalty Levels In The Computer Misuse Legislation Of Britain, Malaysia And Singapore , Computer Law & Security Report Vol. 16 No. 5, 2000.

(18) J. Dianne Brinson, Analyzing E. Commerce & Internet Law, prentice hall PTR, New Jersey, USA, 2001.

(19) Jean Camp, Trust and Risk in internet Commerce, the MIT press, Cambridge, England, 2000.

(20) Joffery F.Beatty & Susan S. Samuelson, Essentials

of Business law, 2nd Edition Thomson, , 2005, p808.

(21) John Bagby ,E, Commerce law (Issues for Business Thomson, South, Western west London , 2003.

(22) Jonathan Rosenar Cyber Law. The law of the internet, ed Springer, 1997.

(23) Keith Harrison, Bill Munro and Tim Spiller, HP Laboratories, Security through uncertainty, Network Security Magazine, February 2007.

(24) L. Jean Camp & D. Riley, "Protecting an unwilling electronic populace", Proceedings of the Fifth Conference of Computers Freedom and Privacy, 28, 31 March 1995, San Francisco, CA.

(25) Lawrence B. Solum and Minn Chung, The Layers Principle: Internet Architecture and the Law, University of San Diego School of Law, Public Law and Legal Theory Research Paper 55

(26) Loma Brazell: Electronic signatures law and regulations. Sweet And Maxwell, London, 2004.

(27) Marshall J. Wech, International protection of intellectual property P. 1, Texas intellectual property journal, the university of Texas school of law, [1, Twx. Intel. Prop, 1, j, 44] 1993.

(28) Minyan Wang &Queen Mary, University of London, Do the regulations on electronic signatures facilitate international electronic commerce? A critical review5, computer law & s e c u r i t y r e p o r t 2 3 , 2 0 0 7..

(29) Mohan Atreya and Benjamin Hammond and Stephen Paine and paul starret and Stephen Wu: Digital signatures, McGraw, Hill\Osborne, New York, 2002.

(30) Ravi kalakota & Andrew B.whinston, Frontiers of

electronic commerce. Addison Wesley publishing 1996.

(31) Reedc: What is a signature?:2000The Journal of information, Law and Technology(JIL "http:www.elj.warwick.ac.uk\jilt\00, 3reed.htmll"

(32) Roger Leroy Miller & Gaylord A.Jentz, Law for Electronic Commerce Thomson Learning, 2000.

(33) Ter Kah Leng, NEW LAWS ON E, COMMERCE" SINGAPORE, Computer Law & Security Report Vol. 15 no. 1 1999.

(34) Thelen Reid & Priest LLP, current legal issues facing business on the internet: legal risks and how they can be avoided ,available online at: http://libraary.lp.Findlaw.com/scripts/getfile.pl?FILE=firms/thelen/thelen/trp00003

(35) Thomas C.Baxter,Jr _ Sephanie A.Heller ,The ABCs of the UCC , Article 4A: Fund Transfer , by the American Bar Association 1997.

(36) Tom forester, Essential problems to High, Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989.

(37) Warwick Ford & Michael S. Baum, Secure Electronic Commerce Building the Infrastructure for Digital Signatures and Encryption, prentice Hall, 'New Jersy 2001.

(38) William E.wyrough. Jr. & Ron Klein, the electronic signature act of 1996: breaking down barriers to widespread electronic commerce I Florida , Florida state university law review.

(39) Yacine Atif, A distributed and interoperable object, oriented support for safe e, commerce transactions, , available at: www.elseviercomuterscience.com

مراجع باللغة الفرنسية

(40) Ander Iucas, le driot de l'informatique henis droit, press universitaitrem frqance, Paris, 1987.

(41) Ben Halima (sass "Les crimes informatiques et d'autre crimes dans le domaine de la tachnologie informatique en Tunisie", R.I.D., 612.

(42) CAPRIOLI Eric A, Preuve et signature dans le commerce electronique, Droit & Patrimoin, n 55, December, 1997.

(43) Catala pierre Ebouche d'une bheonrie duriique de I'information D, S. 1974.

(44) Ceux qui, en connaissance de cause, auront accepte de recevoir un paiement au moyen d une carte de paiement contrefaite ou falsifiee.

(45) CHAPUT (Y, la loi no 91, 1382 du 30 decembre 1991 relative a la securite des cheques et des cartes de paiement; D. S. 1992.

(46) Christiana Feral, Schuhl, Cyber Droit le droit 'a l'epreuve de l'internet, 3 e'dition 2001.

(47) Convention sur la cybercriminalité. STE. no. 185, Rapport explicatif adopte le 8 novembre 2001..

(48) Daniel Martin: La menace de la cybercriminalite, Revue des problemes economiques, n 2706, 28mars2001

(49) Daniel Padoin,la criminalite informatique le role de la police judiciaire gaz pal 1996,Dossier special.

(50) Directive 97\7\CE du Parlement Europeen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matiere de contrats a distance, J.O.C.E.L 144 du 4 juin 1997.

(51) ESPAGNON Michel, La securite des Paiements effectues sur des reseaux ouverts (interne , Problematique juridique generale, in Colloque sur ,

Les novellas pratiques delictuelles liees aux technologies de la communication, Poitiers les 22 et 23 november 1996, Presses universitaires de France, 1999.

(52) ETIENNE MADRANGES, La loi du 30 decembre 1991, relative a la securite des cheques et des cartes de paiement, vers un denengorgement des tribunaux, la novelle penalite Liberatoire, G. P. Doc 1992.

(53) G. Bertin et al., De lambertaire, la proctection du logiciel, en feux juridiques.

(54) Gabriel Roujou De Bauble, Bernard Bouloc, Jacques francillon, Yeves mayavd, CODE PENAL COMMENT, article par article, livres a 5, Dalloz, 1996.

(55) GAVALDA (C, Les cartes de paiement et de credit, DALLOZ, 1994.

(56) GREDOT (F. J Conditions et effets des oppositions en matiere de carte de paiement, petites Affiches l986, no 22.

(57) henri d esbois commerce electronique et proprieties intellectuelles librairies techniques paris 2001.

(58) herman Bekeart, Introduction a L etude de droit Bruxelles, Document du travail, Travaux de L association Henri Capitant T.XXIV , edition 19, 1973.

(59) Heymann (Stephen , Legislating Compyter Crime, H.J.L, 1997, vol.34.

(60) Highlights, National Infrastructure Protection Center, Issue 7, 01 July 15, 2001.

(61) J. L. Coutal: La protection jumidique de logical, dalloz, 1984, Chronique.

(62) J. R. Bonneau: Note sous CA de Paris, 2 Novembre 1982, Gaz. Pal. 3 mars 1983.

(63) Jean Calais, Auloy, Droit de la Consommation, 3e edition 1992.

(64) Jerome Huet, Aspects juridique du telepaiement, JCP, Ed. G., I, 3524, 1991.

(65) L. Jean Camp, Peer to Peer Systems, The Internet Encyclopedia ed. Hossein Bidgoli, John Wiley & Sons (Hoboken, New Jerse 2003..

(66) L. Jean Camp, Trust & Risk in Internet Commerce, MIT Press, Winter (Cambridge, M 2000.

(67) Latteron (Roselin, Le droit a loubli, R.D.P., 1996.

(68) Leclerq (Pierr et Catala (Pierr, L'information est, elle un bien informatique, Masson, 1992.

(69) Lillian Edwards & Charlotte Waelde, law and internet Framework of electronic commerce, HARF publishing Oxford second Edition, 2000

(70) Lionel costs:"Aperçu sur le droit du commerce électronique aux Etats Unis", droit et patrimoine, N 55, décembe 1997.

(71) MARTIN (Didier R, la carte de payement et la loi Ou la puce maltraite, D. S. H., octobre 1992.

(72) Nicole Tortello et Pascal Lointier: Internet pour les jurists, Dalloz, 1996.

(73) Olivier Berthier, Le credit documentaire a l heure d internet, BANQUE magazine, n 639, septembre 2002.

(74) P. Sérielle: La propriété littéraire et droits voisins , Ed Dalloz, 1992.

(75) Peter Schnaitman, Building a Community Through Workplace E, mail: The New Privacy Frontier, 2001 at: http://www.mttlr.org/volfive/schnaitman.html

(76) Pierre Bouzat, La protection penal du consommateur, Lectures a etudes superieures a Faculte du Droit d Alexandria, 1998.

(77) R. Plasisant: La loi N 85, 660 du 3 juillet 1985 relative aux droits d'auteur ètaux droits des artistes , interprétées , des producteurs de phonogrammes et de v idéogrammes et des inter prises de communications audiovisuelles , JCP , 1986 , 1 , Doct., 3230

(78) Raymond Thomas, Introduction Generale, 81 Congres des Notaires de France, Le Consommateur, Tome I, Lyon, 12, 15 Mai 1985

(79) Real - life Corpoate Domain Name challenges, Issues and strategic Solution Available at: www.verisign.com

(80) Richard Milchir , Marques et Noms De domain de quelques Problemes Actuels.lamy droit commercial. No 135. juillet. 2000. Bulletin d'actualite.

(81) SALAUN Anne, Les Paiements electroniques au regard de la vente a distance, Droit de l informatique et des Telecoms, n 99..

(82) Steven Furnell, E, commerce security a question of trust, Computer fraud& security Magazine.

(83) T. delugo, La Legislation penala & son application, Uni. De Caire 1956.

(84) YVES GUYON, Droit des affaires, TI: Droit commercial generale et societes, 9 ed., ECONOMICA, 1996, n 78.

مواقع الإنترنت:

(85) http// www.msh, paris.fr/red&s/index.htm

(86) http//www.gmd.de/people/herbert.burkert/rom. htm

(87) http: // www et. 8m. com / virusty pes. htm

(88) http: //www. Asiasource. Org\news

(89) http: //www. Naavio.org\importlaws\itbill2000\preamble. htm

(90) http:// safola.com/signature.chtml

(91) http:// www. Bakernet. Com\ ecommerce\ japan, t.htm

(92) http:// www.eb. 8m.com/virustypes, htm

(93) http:// www.iascrow.com

(94) http:// www.islamonline.net/iol, arabic/dowalia/scince, 14/ dcincel.asp

(95) http://2163.11671/ipw/articles/ipwa01.htm

(96) http://ar.wikipedia.org/wiki/

(97) http://arabic.mjustice.dz/liguearabe/loi_emir_ar_crim_tech_info/loi_e mir_ar_crim_tech_info.htm

(98) http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

(99) http://ecommerce.wipo.int/databases/trademark/index.htm l

(100) http://forum.stop55.com/112298.html

(101) http://forum.stop55.com/86370.html

(102) http://jya.com/eu, difsig3.htm

(103) http://news.bbc.co.uk/hi/arabic/sci, tech/newsid, 3359000/3359369.stm

(104) http://slr.stanford.edu/stlr/articles/99strl1/index.htm

(105) http://vb.mixxat.com/t9878.html

(106) http://www. Bakernet.com\ecommerce\Malaysia, t, summary. htm

(107) http://www.alarabiya.net/views/2005/06/25/14298.html

(108) http://www.albayan.co, ae/albayan/2000/07/01/ola/4.htm

(109) http://www.aleqt.com/2009/01/15/article_184514.html

(110) http://www.alkhaleej.ae/portal/84ce079b-52fa-4285-8c1a-60ac348633ad.aspx

http://www.anageed.com/vb/archive/index.php/t.

10008.html

(112) http://www.arabcin.net.

(113) http://www.arabelect.net/stories/149.htm

(114) http://www.arabianbusiness.com/arabic/552868

(115) http://www.bintnet.com/club/showthread.php?t=33709

(116) http://www.cybercrime.gov/haltinnerSent.pdf

(117) http://www.cybercrime.gov/homeland_CSEA.htm

(118) Http://Www.Cybercrime.Gov/Tandiwidjojosent.Pdf

(119) http://www.egyptatwsis.com.eg/ar/Partners.asp

(120) http://www.elaph.com/Web/Technology/2009/4/433295.htm

(121) http://www.emaratalyoum.com

(122) http://www.emaratalyoum.com/Articles/2008/11/Pages/11272008_6fe1a8d51e3244c7bac8afd11c4815c0.aspx

(123) http//:www.gmd.de/people/herbert.burkert/rom. htm

(124) http://www.grolier.fr/cyberlexnet/com/a98099902.htm

(125) http://www.gseis.ucla.edu/iclp/internet.html

(126) http://www.icann.org/tr/arabic.html

(127) http://www.ict.gov.qa/output/NewsPage.aspx?PageID=868

(128) http://www.ipsterraviva.net/TV/tunis/printArabic.asp?idnews=21

(129) http://www.itep.ae/Arabic/EducationalCenter/Articles/Extranet_01.asp

(130) http://www.itu.int/net/home/index, ar.aspx

(131) http://www.itu.int/wsis/indexar.html

(132) http://www.juriscom.net/chr/1/fr19980710.htm

(133) http://www.legalis.net/jnetldecisions/marques/tgi_nanterre_srf.htm

(134) http://www.losha.net/vb/showthread.php?t=425.

(135) http://www.maddawi.net/book

(136) http://www.marefa.org

(137) http://www.microsoft.com/presspass/features/2000/ceosummit/os, 24gates.asp

(138) http://www.middle,east,online.com/Tech/jan2001/internetprivacy 2/2/2001 htm.

(139) http://www.middle, east, online.com/technology/?id=22726

(140) http://www.computerconomics.com

(141) http://www.msh, parist.fr/red&s/index.htm

(142) http://www.oyez.org/cases/1990, 1999/1996/1996_96_511/

(143) http://www.saudistocks.com/forums/saudi9/stocks312473

(144) http://www.startimes2.com/f.aspx

(145) http://www.swissinfo.org/ara/news/science_technology.html? siteSect=511&sid=4458716&cKey=1070636924000&ty=st

(146) http://www.thegulfbiz.com/archive/index.php/t, 1544.html

(147) http://www.trade.direct.com

(148) http://www.uaeec.com/news-action-show-id-18787.htm

(149) http://www.un.org/arabic/conferences/wsis/faq3.htm

(150) http://www.uncitral.org

(151) http://www.uplink.com.au/lawlibrary/document/docs/doc32.htm

(152) http://www.utexas.edu/law/journals/tipilj/vollissI/welch.htm.SECI

(153) http://www.uwhois.com.

(154) http://www.wipo.int/pressroom/ar/articles/2008/artic

le_0015.html#table1

(155) http://www.wipo.int/sme/ar/e_commerce/domain_names.htm

(156) http://www.wipo.org

(157) http:/www.eg.astate.et.us/2000/rpt/oir/htm/2000, 1, 0795.htm

(158) www.aflajgedu.gov.sa/vb/showthread.php?t=9341

(159) www.albawaba.com/ar/literature,lterary_lnalysis/276136

(160) www.albawaba.com/ar/literature,lterary_lnalysis/276136

(161) www.arab ency.com / index.php?module=pnEncyclopedia&func =display_term&id=159758 1 (rataments by Bill Gates. Redmond wash may 24 2000. Press pass, microsoft page. Available onolin in june 2000 at:

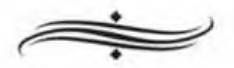
(162) www.cybercrime.gov/coedraft.html

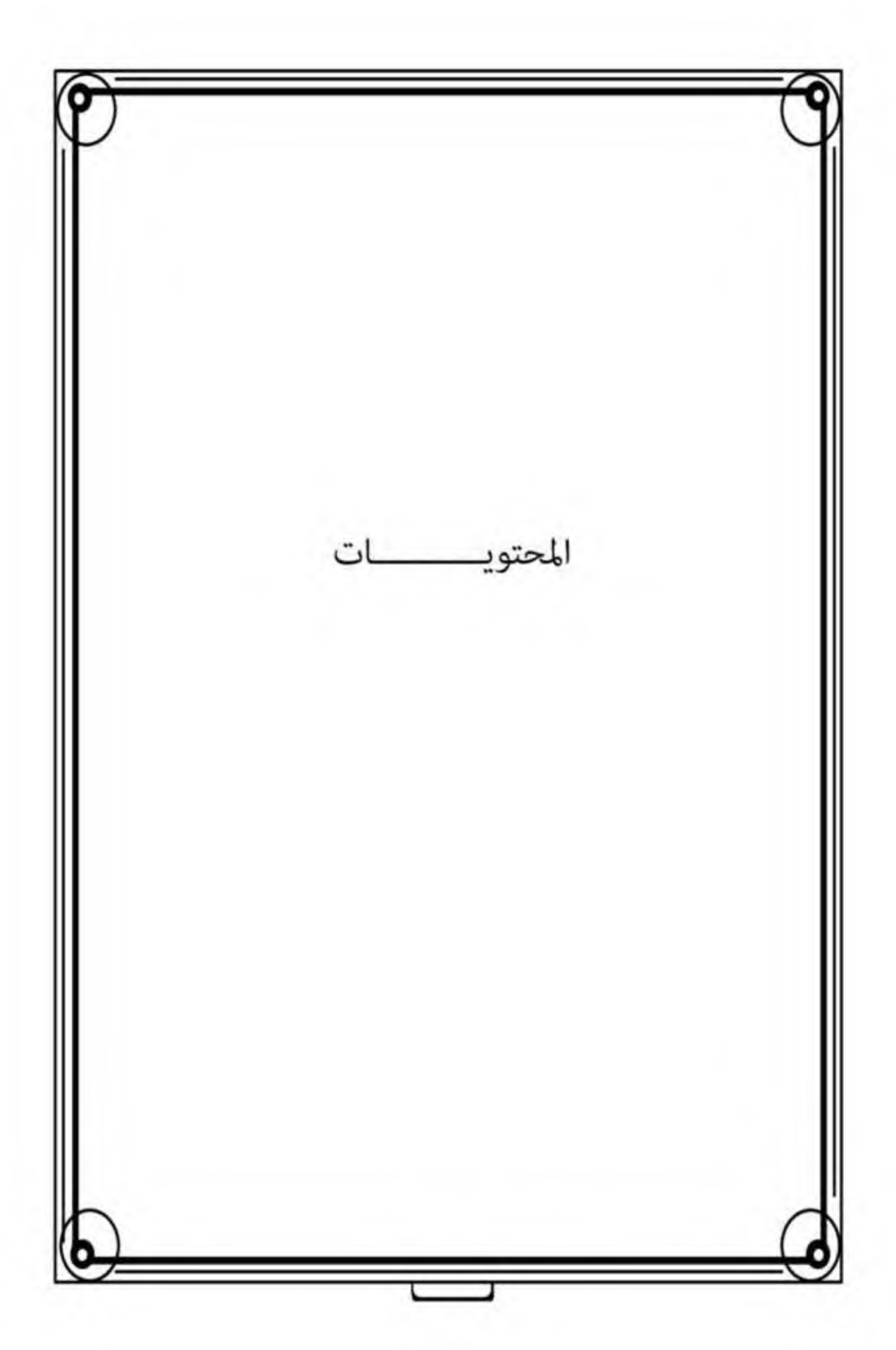
(163) www.iitf.nist.gov/eleccomm/ecomm.htm

(164) www.megaclub.gov.eg/Content/Default.aspx

(165) www.tashreaat.com/view_studies2.asp?id=288std_id=66

(166) www.uqu.edu.sa/mypage/drabid/ecommerce1.htm





المحتويـــــات

المحتويات

الموضـــــوع	الصفحة

الفصل التمهيدي

التنظيم القانوني للإنترنت

الباب الأول

أساسيات التجارة الإلكترونية وحمايتها

المستشار الدكتور محمد عبيد الكعبي

المؤهلات العلمية:-

- دكتوراه في الحقوق (القانون الجنائي) من جامعة القاهرة.
- ماجستير في الحقوق (القانون الجنائي) من جامعة القاهرة.
- دبلوم القانون الجنائي من جامعة عين شمس.
- ليسانس الشريعة والقانون من جامعة الإمارات العربية المتحدة.

المؤهلات العملية:-

- الدفعة الأولى لمعهد التدريب والدراسات القضائية بدولة الإمارات العربية المتحدة.
- عمل وكيلا للنائب العام ثم وكيل أول نيابة ثم رئيساً للنيابة العامة.
- عمل قاضيا ثم رئيس محكمة.
- رئيساً لقسم البحوث والدراسات بمعهد التدريب والدراسات القضائية سابقا.
- عضو الهيئة التدريسية وأستاذ محاضر بمعهد التدريب والدراسات القضائية.

اللجان المشارك بها:-

- لجنة إعداد مشروع قانون عربي استرشادي حول التجارة الالكترونية.
- لجنة إعداد قانون عربي استرشادي للإثبات بالوسائل الحديثة.
- لجنة الخبراء المختصين بمناقشة مشروع القانون الموحد لمكافحة جرائم تقنية المعلومات لدول الخليج العربي.
- لجنة إعداد مشروع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.



الكتب والبحوث والمقالات:-

- الحماية الجنائية للتجارة الالكترونية.
- أضواء على قانون مكافحة جرائم تقنية المعلومات الإماراتي.
- حماية الخصوصية عبر الانترنت.
- الدخول غير المشروع على المواقع والأنظمة المعلوماتية.
- سرقة المعلومات بين الإباحة والتجريم.
- جريمة النصب والاحتيال عبر الانترنت.
- المجرم المعلوماتي.

دار النهضة العربية للنشر والتوزيع